OSY.SSI[2015][11]

Attack planning

Question

Attack planning

a.k.a. the Starcraft God Mode lecture.

If you understand how attacks work...

Attack planning

a.k.a. the Starcraft God Mode lecture.

If you understand how attacks work...
...you may be less clueless about defences.

Attack planning

a.k.a. the Starcraft God Mode lecture.

If you understand how attacks work...
...you may be less clueless about defences.
...you may leverage the same techniques elsewhere.

Attack planning

a.k.a. the Starcraft God Mode lecture.

If you understand how attacks work...
...you may be less clueless about defences.
...you may leverage the same techniques elsewhere.

Also more and more certifications *require* you to attack yourself.

Table of Contents

Strategic layer cake

Strategic levels

"Means to an end".

Strategic layer cake

Strategic levels

"Means to an end".

Organised by distance:

- How do we destroy/compromise X?

Strategic layer cake

Strategic levels

"Means to an end".

Organised by distance:

- How do we destroy/compromise X? "Operational".

Strategic layer cake

Strategic levels

"Means to an end".

Organised by distance:

- How do we destroy/compromise X? "Operational".
- How do we get to/subvert X?

Strategic layer cake

Strategic levels

"Means to an end".

Organised by distance:

- How do we destroy/compromise X? "Operational".
- How do we get to/subvert X? "Tactical".

Strategic layer cake

Strategic levels

"Means to an end".

Organised by distance:

- How do we destroy/compromise X? "Operational".
- How do we get to/subvert X? "Tactical".
- What kind of X do we want?

Strategic layer cake

Strategic levels

"Means to an end".

Organised by distance:

- How do we destroy/compromise X? "Operational".
- How do we get to/subvert X? "Tactical".
- What kind of X do we want? "Strategic".

Strategic layer cake

Strategic levels

"Means to an end".

Organised by distance:

- How do we destroy/compromise X? "Operational".
- How do we get to/subvert X? "Tactical".
- What kind of X do we want? "Strategic".
- What do we want?

Strategic layer cake

Strategic levels

"Means to an end".

Organised by distance:

- How do we destroy/compromise X? "Operational".
- How do we get to/subvert X? "Tactical".
- What kind of X do we want? "Strategic".
- What do we want? "Political"/Philosophical/Ideological.

Strategic layer cake

Strategic levels

"Means to an end".

Organised by distance:

- How do we destroy/compromise X? "Operational".
- How do we get to/subvert X? "Tactical".
- What kind of X do we want? "Strategic".
- What do we want? "Political"/Philosophical/Ideological.

No clear distinctions, but helpful model.

Strategic layer cake

Soldiers

Strategic layer cake

Soldiers

Last time: operational knowledge..

Strategic layer cake

Soldiers

Last time: operational knowledge..

Example of operation :

- send a crafted packet to a server,

Strategic layer cake

Soldiers

Last time: operational knowledge..

Example of operation :

- send a crafted packet to a server,
- cause a buffer overflow,

Strategic layer cake

Soldiers

Last time: operational knowledge..

Example of operation :

- send a crafted packet to a server,
- cause a buffer overflow,
- use ROP to escalate priviledges

Strategic layer cake

Soldiers

Last time: operational knowledge..

Example of operation :

- send a crafted packet to a server,
- cause a buffer overflow,
- use ROP to escalate priviledges
- get control of the server

Strategic layer cake

Soldiers

Last time: operational knowledge..

Example of operation :

- send a crafted packet to a server,
- cause a buffer overflow,
- use ROP to escalate priviledges
- get control of the server
- send packet from the server to another server

Strategic layer cake

Captains and lieutenants

Strategic layer cake

Captains and lieutenants

Example of tactical operation:

Strategic layer cake

Captains and lieutenants

Example of tactical operation:

- Use disguise to seduce the nerdy IT guy,

Strategic layer cake

Captains and lieutenants

Example of tactical operation:

- Use disguise to seduce the nerdy IT guy,
- Plug an USB key to exploit his Mac AirBook

Strategic layer cake

Captains and lieutenants

Example of tactical operation:

- Use disguise to seduce the nerdy IT guy,
- Plug an USB key to exploit his Mac AirBook
- Evade by claiming you have to go to the WC and get out of the building

Strategic layer cake

Captains and lieutenants

Example of tactical operation:

- Use disguise to seduce the nerdy IT guy,
- Plug an USB key to exploit his Mac AirBook
- Evade by claiming you have to go to the WC and get out of the building
- Exfiltrate data from company to HQ.

Strategic layer cake

Generals and commanders

Strategic layer cake

Generals and commanders

Example of strategic operation

Strategic layer cake

Generals and commanders

Example of strategic operation

- Ruin the reputation of Gesu Yarō Corp.

Strategic layer cake

Generals and commanders

Example of strategic operation

- Ruin the reputation of Gesu Yarō Corp.
- Reveal the affair of Mr Húndàn with Mrs Jìnǚ.

Strategic layer cake

Generals and commanders

Example of strategic operation

- Ruin the reputation of Gesu Yarō Corp.
- Reveal the affair of Mr Húndàn with Mrs Jìnǚ.
- Block production of Feind GmbH.

Strategic layer cake

Generals and commanders

Example of strategic operation

- Ruin the reputation of Gesu Yarō Corp.
- Reveal the affair of Mr Húndàn with Mrs Jìnǚ.
- Block production of Feind GmbH.
- False flag Porochny Inc.

Strategic layer cake

Chiefs

Strategic layer cake

Chiefs

Example of political goals:

Strategic layer cake

Chiefs

Example of political goals:

- Become world leader in consulting

Strategic layer cake

Chiefs

Example of political goals:

- Become world leader in consulting
- But be subtle! And no killing. (“doctrine”)

Strategic layer cake

Chiefs

Example of political goals:

- Become world leader in consulting
- But be subtle! And no killing. (“doctrine”)

The strategic question

Recursively:

The strategic question

Recursively:

- given "vague" or "global" objective Y,

The strategic question

Recursively:

- given "vague" or "global" objective Y,
- what "concrete" or "local" objectives X should we target and how

The strategic question

Recursively:

- given "vague" or "global" objective Y,
- what "concrete" or "local" objectives X should we target and how

Examples: chess, Go, robotic motion, etc.

Example: the Botnet Master Equation

Example: the Botnet Master Equation

Data:

Example: the Botnet Master Equation

Data:

- w_i: work necessary to compromise host i

Example: the Botnet Master Equation

Data:

- w_i: work necessary to compromise host i
- r_i: risk of getting caught while attacking i

Example: the Botnet Master Equation

Data:

- w_i: work necessary to compromise host i
- r_i: risk of getting caught while attacking i
- π_i: work generated by i once compromised

Example: the Botnet Master Equation

Data:

- w_i: work necessary to compromise host i
- r_i: risk of getting caught while attacking i
- π_i: work generated by i once compromised

Goal: find the optimal sequence $i_1, i_2, \ldots$ of targets, to infect a maximum of host in a given time.

Textbook case: knapsack

Textbook case: knapsack

A thief gets in a jewelry with a knapsack. Each jewel has

Textbook case: knapsack

A thief gets in a jewelry with a knapsack. Each jewel has

- A value v_i

Textbook case: knapsack

A thief gets in a jewelry with a knapsack. Each jewel has

- A value v_i
- A weight w_i

Textbook case: knapsack

A thief gets in a jewelry with a knapsack. Each jewel has

- A value v_i
- A weight w_i

The knapsack can only carry a weight W.

Textbook case: knapsack

A thief gets in a jewelry with a knapsack. Each jewel has

- A value v_i
- A weight w_i

The knapsack can only carry a weight W.

What items do you choose?

Computer-assisted attacks

Fact: we won't refrain from using computers to help planning attacks.

Your attackers won't either.

Table of Contents

How are attacks planned?

A few standard steps:

How are attacks planned?

A few standard steps:

1. Target identification and reconnaissance

How are attacks planned?

A few standard steps:

1. Target identification and reconnaissance
2. Vulnerability discovery

How are attacks planned?

A few standard steps:

1. Target identification and reconnaissance
2. Vulnerability discovery
3. Exploit weaponisation

How are attacks planned?

A few standard steps:

1. Target identification and reconnaissance
2. Vulnerability discovery
3. Exploit weaponisation
4. Payload delivery

How are attacks planned?

A few standard steps:

1. Target identification and reconnaissance
2. Vulnerability discovery
3. Exploit weaponisation
4. Payload delivery
5. Evasion

How are attacks planned?

A few standard steps:

1. Target identification and reconnaissance
2. Vulnerability discovery
3. Exploit weaponisation
4. Payload delivery
5. Evasion
6. Goto 1.

How are attacks planned?

A few standard steps:

1. Target identification and reconnaissance
2. Vulnerability discovery
3. Exploit weaponisation
4. Payload delivery
5. Evasion
6. Goto 1.

Again, no sharp frontiers, but a useful roadmap.

0. War

0. War

"Maximise freedom of movement"

1. Target identification and reconnaissance

Know thy enemy

- Goal:

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"
  - Identify what to do with it (destruction, disruption, degradation, seizure, neutralization, exploitation...)

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"
  - Identify what to do with it (destruction, disruption, degradation, seizure, neutralization, exploitation...)
- Means:

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"
  - Identify what to do with it (destruction, disruption, degradation, seizure, neutralization, exploitation...)
- Means: OSINT, investigation, mapping (sat, net), HUMINT, surveillance

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"
  - Identify what to do with it (destruction, disruption, degradation, seizure, neutralization, exploitation...)
- Means: OSINT, investigation, mapping (sat, net), HUMINT, surveillance
- Cost:

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"
  - Identify what to do with it (destruction, disruption, degradation, seizure, neutralization, exploitation...)
- Means: OSINT, investigation, mapping (sat, net), HUMINT, surveillance
- Cost: Low (OSINT) to high (HUMINT)

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"
  - Identify what to do with it (destruction, disruption, degradation, seizure, neutralization, exploitation...)
- Means: OSINT, investigation, mapping (sat, net), HUMINT, surveillance
- Cost: Low (OSINT) to high (HUMINT)
- Risk:

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"
  - Identify what to do with it (destruction, disruption, degradation, seizure, neutralization, exploitation...)
- Means: OSINT, investigation, mapping (sat, net), HUMINT, surveillance
- Cost: Low (OSINT) to high (HUMINT)
- Risk: Low risk

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"
  - Identify what to do with it (destruction, disruption, degradation, seizure, neutralization, exploitation...)
- Means: OSINT, investigation, mapping (sat, net), HUMINT, surveillance
- Cost: Low (OSINT) to high (HUMINT)
- Risk: Low risk
- Time:

1. Target identification and reconnaissance

Know thy enemy

- Goal: Search for interesting targets:
  - Targets' compromission should further your goal (politically, strategically, ...)
  - Start a broad selection (surveillance), then refine (recon)
  - The main point is to select targets where success is "100% assured"
  - Identify what to do with it (destruction, disruption, degradation, seizure, neutralization, exploitation...)
- Means: OSINT, investigation, mapping (sat, net), HUMINT, surveillance
- Cost: Low (OSINT) to high (HUMINT)
- Risk: Low risk
- Time: unconstrained/weakly constrained

1. Target identification and reconnaissance

What are we interested in?

1. Target identification and reconnaissance

What are we interested in?

- Value:

1. Target identification and reconnaissance

What are we interested in?

- Value: Background information, activity, symbolic value, media attention, ...

1. Target identification and reconnaissance

What are we interested in?

- Value: Background information, activity, symbolic value, media attention, ...
- Flows:

1. Target identification and reconnaissance

What are we interested in?

- Value: Background information, activity, symbolic value, media attention, ...
- Flows: Routines, transportation, personnel actual and past...

1. Target identification and reconnaissance

What are we interested in?

- Value: Background information, activity, symbolic value, media attention, ...
- Flows: Routines, transportation, personnel actual and past...
- Situation:

1. Target identification and reconnaissance

What are we interested in?

- Value: Background information, activity, symbolic value, media attention, ...
- Flows: Routines, transportation, personnel actual and past...
- Situation: Location, history, collaterals and linkage, position in a system, critical nodes...

1. Target identification and reconnaissance

What are we interested in?

- Value: Background information, activity, symbolic value, media attention, ...
- Flows: Routines, transportation, personnel actual and past...
- Situation: Location, history, collaterals and linkage, position in a system, critical nodes...
- Visibility:

1. Target identification and reconnaissance

What are we interested in?

- Value: Background information, activity, symbolic value, media attention, ...
- Flows: Routines, transportation, personnel actual and past...
- Situation: Location, history, collaterals and linkage, position in a system, critical nodes...
- Visibility: observational outposts to check for change and assess attack success

1. Target identification and reconnaissance

What are we interested in?

- Value: Background information, activity, symbolic value, media attention, ...
- Flows: Routines, transportation, personnel actual and past...
- Situation: Location, history, collaterals and linkage, position in a system, critical nodes...
- Visibility: observational outposts to check for change and assess attack success

Find an example!

2. Vulnerability discovery

Know thy enemy's weakness

- Goal:

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission
- Means:

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission
- Means: analysts, replication, reverse-engineering, scanning, fuzzing...

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission
- Means: analysts, replication, reverse-engineering, scanning, fuzzing...
- Cost:

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission
- Means: analysts, replication, reverse-engineering, scanning, fuzzing...
- Cost: Low (fuzzing) to high (0-day)

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission
- Means: analysts, replication, reverse-engineering, scanning, fuzzing...
- Cost: Low (fuzzing) to high (0-day)
- Risk:

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission
- Means: analysts, replication, reverse-engineering, scanning, fuzzing...
- Cost: Low (fuzzing) to high (0-day)
- Risk: Low (off-line) to medium (on-line)

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission
- Means: analysts, replication, reverse-engineering, scanning, fuzzing...
- Cost: Low (fuzzing) to high (0-day)
- Risk: Low (off-line) to medium (on-line)
- Time:

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission
- Means: analysts, replication, reverse-engineering, scanning, fuzzing...
- Cost: Low (fuzzing) to high (0-day)
- Risk: Low (off-line) to medium (on-line)
- Time: Constrained by target's change cycle

2. Vulnerability discovery

Know thy enemy's weakness

- Goal: knowing the target and what to do to it, find how to achieve that goal
  - Check for access control holes, software or hardware mishaps, human help...
  - The more you know about the target, the easier it is
  - Weaponeering assessment: determine the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage.
  - Attack graph: analyse movements after initial target compromission
- Means: analysts, replication, reverse-engineering, scanning, fuzzing...
- Cost: Low (fuzzing) to high (0-day)
- Risk: Low (off-line) to medium (on-line)
- Time: Constrained by target's change cycle

Good news: targets can't change too fast too often! (Why?)

3. Exploit weaponisation

Minimise operational risk

- Goal:

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction
  - Prepare weapons and logistics of delivery

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction
  - Prepare weapons and logistics of delivery
- Means:

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction
  - Prepare weapons and logistics of delivery
- Means: testing/rehearsal/drills

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction
  - Prepare weapons and logistics of delivery
- Means: testing/rehearsal/drills
- Cost:

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction
  - Prepare weapons and logistics of delivery
- Means: testing/rehearsal/drills
- Cost: Low to medium

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction
  - Prepare weapons and logistics of delivery
- Means: testing/rehearsal/drills
- Cost: Low to medium
- Risk:

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction
  - Prepare weapons and logistics of delivery
- Means: testing/rehearsal/drills
- Cost: Low to medium
- Risk: Low (off-line) to medium (on-line)

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction
  - Prepare weapons and logistics of delivery
- Means: testing/rehearsal/drills
- Cost: Low to medium
- Risk: Low (off-line) to medium (on-line)
- Time:

3. Exploit weaponisation

Minimise operational risk

- Goal: tailor the selected weapons to the selected target
  - Take into account possible intel mistakes, unexpected change, weapon malfunction
  - Prepare weapons and logistics of delivery
- Means: testing/rehearsal/drills
- Cost: Low to medium
- Risk: Low (off-line) to medium (on-line)
- Time: Constrained by target's change cycle

4. Payload delivery

Fire in the hole!

- Goal:

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)
  - Use knowledge gathered in Step 1 to devise the best strategy

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)
  - Use knowledge gathered in Step 1 to devise the best strategy
- Means:

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)
  - Use knowledge gathered in Step 1 to devise the best strategy
- Means: Operatives, (spear)phishing, dragnet, ...

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)
  - Use knowledge gathered in Step 1 to devise the best strategy
- Means: Operatives, (spear)phishing, dragnet, ...
- Cost:

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)
  - Use knowledge gathered in Step 1 to devise the best strategy
- Means: Operatives, (spear)phishing, dragnet, ...
- Cost: Low (untargeted) to high (very targeted)

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)
  - Use knowledge gathered in Step 1 to devise the best strategy
- Means: Operatives, (spear)phishing, dragnet, ...
- Cost: Low (untargeted) to high (very targeted)
- Risk:

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)
  - Use knowledge gathered in Step 1 to devise the best strategy
- Means: Operatives, (spear)phishing, dragnet, ...
- Cost: Low (untargeted) to high (very targeted)
- Risk: Medium to high

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)
  - Use knowledge gathered in Step 1 to devise the best strategy
- Means: Operatives, (spear)phishing, dragnet, ...
- Cost: Low (untargeted) to high (very targeted)
- Risk: Medium to high
- Time:

4. Payload delivery

Fire in the hole!

- Goal: use the prepared weapons to deliver the desired effect
  - Usually direct effect or a payload (RAT, ...)
  - Use knowledge gathered in Step 1 to devise the best strategy
- Means: Operatives, (spear)phishing, dragnet, ...
- Cost: Low (untargeted) to high (very targeted)
- Risk: Medium to high
- Time: Constrained by target's discovery

5. Evasion

Oh boy oh boy oh boy

- Goal:

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!
  - You leave a trail that can betray you

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!
  - You leave a trail that can betray you
- Means:

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!
  - You leave a trail that can betray you
- Means: log erasure, forging/false flag/fake certificates, obfuscated communications...

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!
  - You leave a trail that can betray you
- Means: log erasure, forging/false flag/fake certificates, obfuscated communications...
- Cost:

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!
  - You leave a trail that can betray you
- Means: log erasure, forging/false flag/fake certificates, obfuscated communications...
- Cost: Medium

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!
  - You leave a trail that can betray you
- Means: log erasure, forging/false flag/fake certificates, obfuscated communications...
- Cost: Medium
- Risk:

5. Evasion

Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!
  - You leave a trail that can betray you
- Means: log erasure, forging/false flag/fake certificates, obfuscated communications...
- Cost: Medium
- Risk: Medium (undetected) to high (detected)

5. Evasion

Oh boy oh boy oh boy

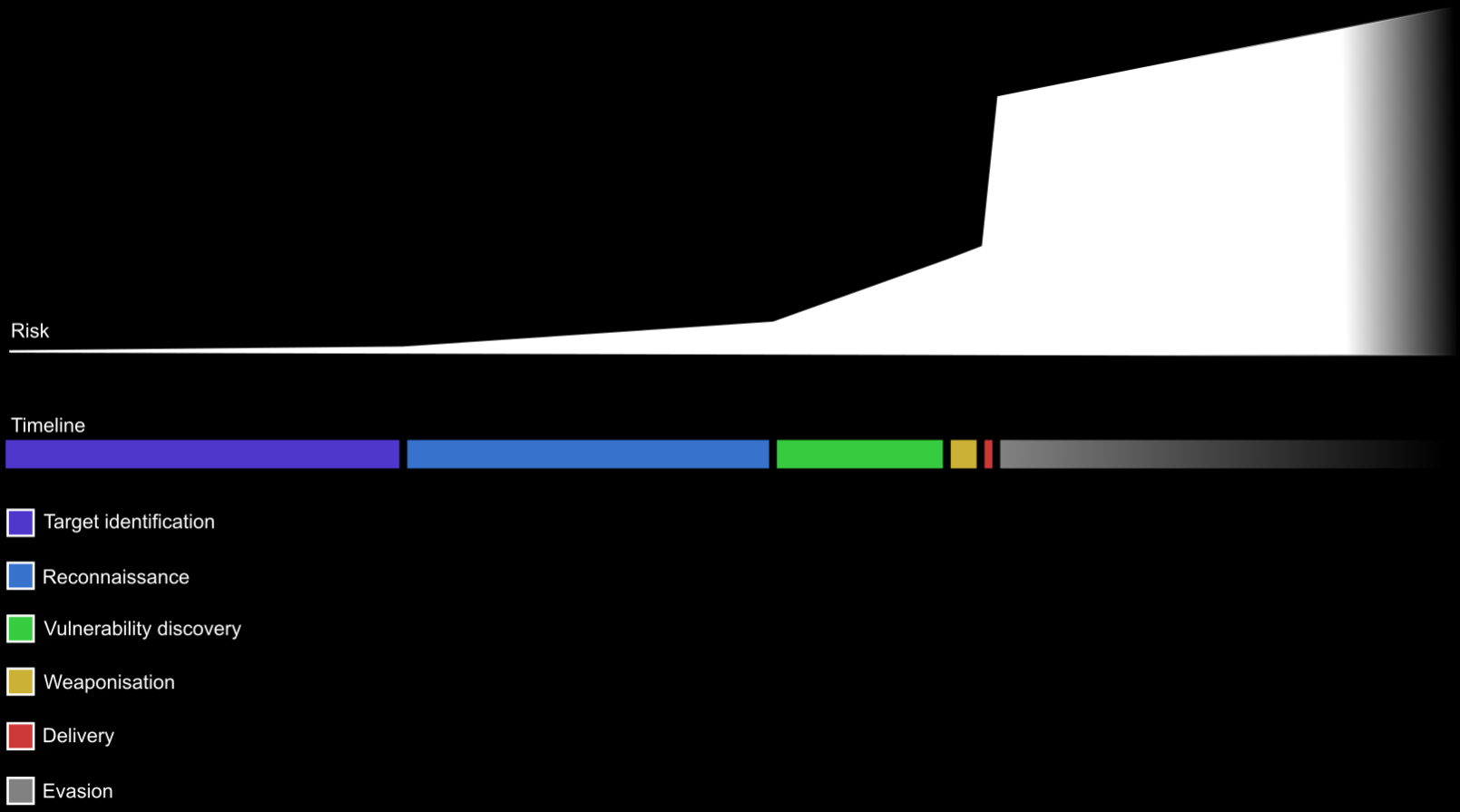
- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!
  - You leave a trail that can betray you
- Means: log erasure, forging/false flag/fake certificates, obfuscated communications...
- Cost: Medium
- Risk: Medium (undetected) to high (detected)
- Time:

5. Evasion

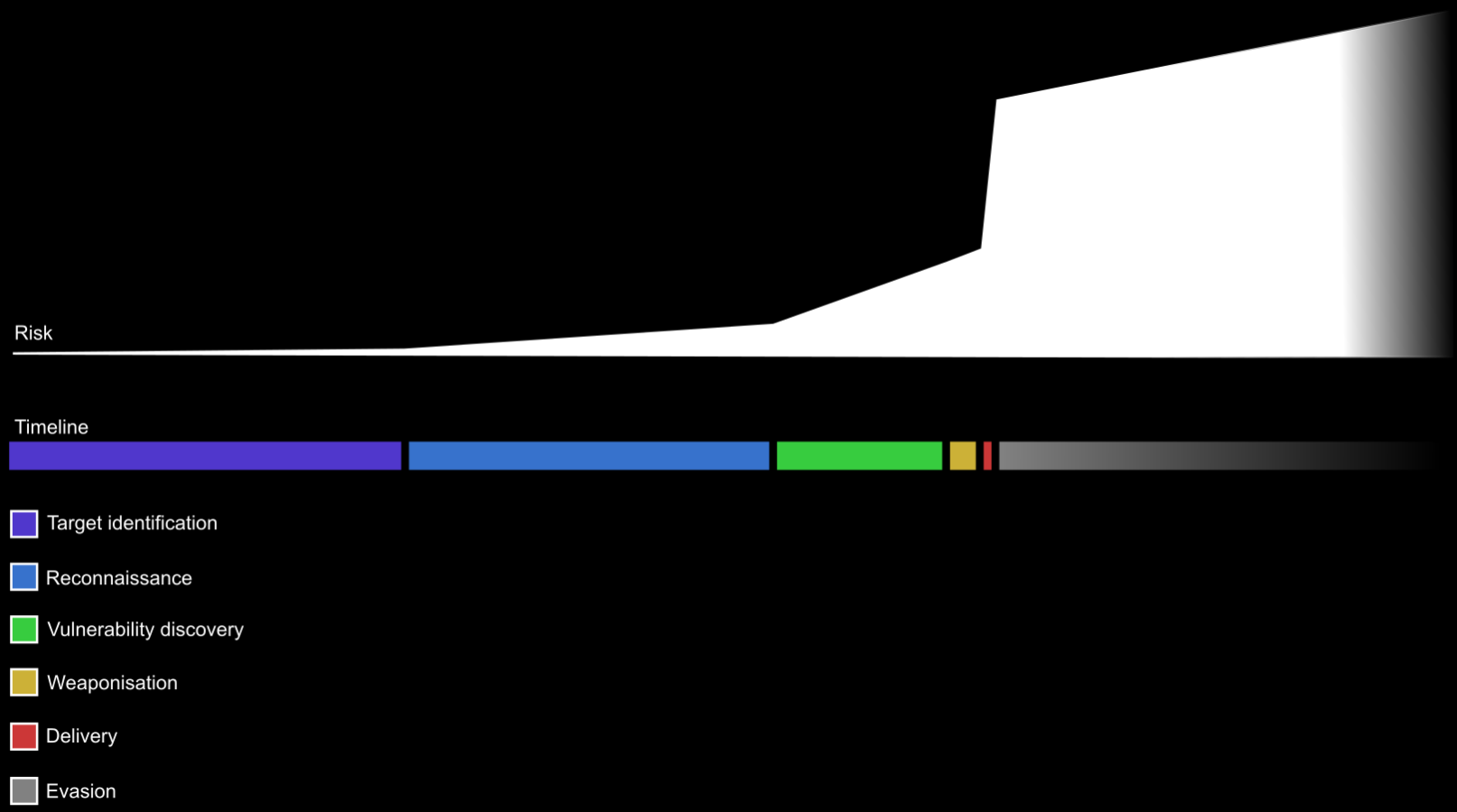
Oh boy oh boy oh boy

- Goal: get away and erase all evidence of operation
  - If the operation isn't detected, evasion isn't necessary
  - If you know you can't get away, put the blame on someone else!
  - You leave a trail that can betray you
- Means: log erasure, forging/false flag/fake certificates, obfuscated communications...
- Cost: Medium
- Risk: Medium (undetected) to high (detected)
- Time: constrained to critically constrained (if detected)

Attack timeline



Attack timeline



Note: A failed operation puts further operations at risk.

Attack timeline

RSA SecurID attack (2011)

28/02

CVE-2011-0609
(@yuange1975)

CVE-2011-0609
Poison Ivy RAT

2011 Recrutement Plan.xls

01/03

Mail to employee 1

02/03

Mail to employee 2

Employee 2 opens it

03/03 to 10/03

Analyses user list and priviledges, bypasses defence in depth mechanisms

Gains access to staging servers

Gains access to server of interest, moves data to staging servers

Compresses and encrypts data, FTP transfer to an external compromised server

Deletes data from there

10/03

EMC/RSA discover the attack, conduct forensics analysis and report to EMC executives

11/03 to 17/03

RSA contacts SecurID customers individually under NDA (~25 000 customers)

17/03

Official SEC 8-K breach declaration

Attack timeline

RSA SecurID attack (2011) – cont'd

Attack timeline

RSA SecurID attack (2011) – cont'd

- 14/03: Adobe Security Advisory admitting the vulnerability

Attack timeline

RSA SecurID attack (2011) – cont'd

- 14/03: Adobe Security Advisory admitting the vulnerability
- 21/03: Adobe Patch

Attack timeline

RSA SecurID attack (2011) – cont'd

- 14/03: Adobe Security Advisory admitting the vulnerability
- 21/03: Adobe Patch
- 27/05: Lockheed Martin attack *using stolen RSA material*

Attack timeline

RSA SecurID attack (2011) – cont'd

- 14/03: Adobe Security Advisory admitting the vulnerability
- 21/03: Adobe Patch
- 27/05: Lockheed Martin attack *using stolen RSA material*
- 31/05: L-3 Communications attack *using stolen RSA material*

Attack timeline

RSA SecurID attack (2011) – cont'd

- 14/03: Adobe Security Advisory admitting the vulnerability
- 21/03: Adobe Patch
- 27/05: Lockheed Martin attack *using stolen RSA material*
- 31/05: L-3 Communications attack *using stolen RSA material*
- 01/06: Northrop Grumman attack *using stolen RSA material*

Attack timeline

RSA SecurID attack (2011) – cont'd

- 14/03: Adobe Security Advisory admitting the vulnerability
- 21/03: Adobe Patch
- 27/05: Lockheed Martin attack *using stolen RSA material*
- 31/05: L-3 Communications attack *using stolen RSA material*
- 01/06: Northrop Grumman attack *using stolen RSA material*
- 06/06: RSA admits SecurID compromise ($66 million loss)

Attack timeline

RSA SecurID attack (2011) – cont'd

- 14/03: Adobe Security Advisory admitting the vulnerability
- 21/03: Adobe Patch
- 27/05: Lockheed Martin attack *using stolen RSA material*
- 31/05: L-3 Communications attack *using stolen RSA material*
- 01/06: Northrop Grumman attack *using stolen RSA material*
- 06/06: RSA admits SecurID compromise ($66 million loss)
- 01/12: 0 detections on VirusTotal

Attack timeline

Direction of movement

- Vertical movement: gaining access to more critical areas
- Horizontal movement: gaining access to neighbouring areas

Attack graph

Real attacks coordinate *multiple vulnerabilities*.

Attack graph

Real attacks coordinate *multiple vulnerabilities*.

Attackers can maintain activity *as long as they're not caught*.

Attack graph

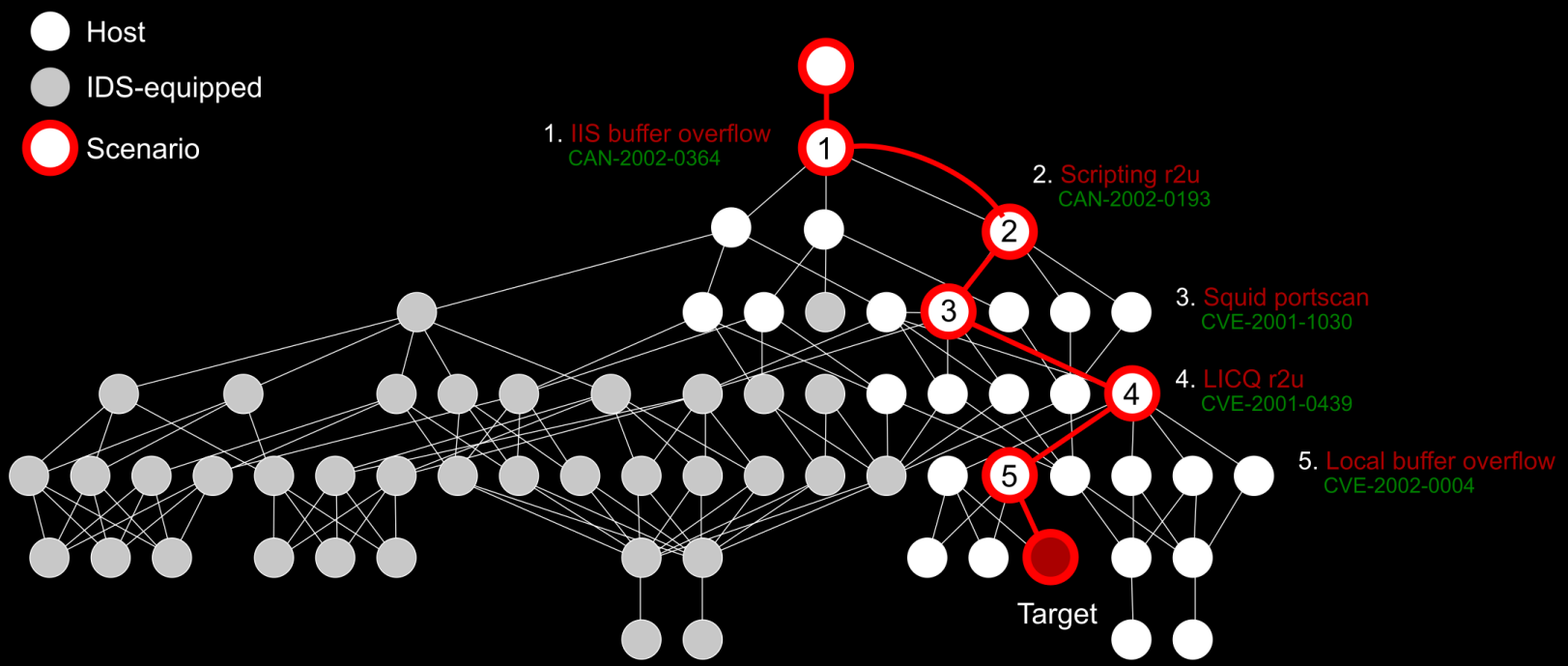
Real attacks coordinate *multiple vulnerabilities*.

Attackers can maintain activity *as long as they're not caught*.

Advanced Persistent Threats (APT).

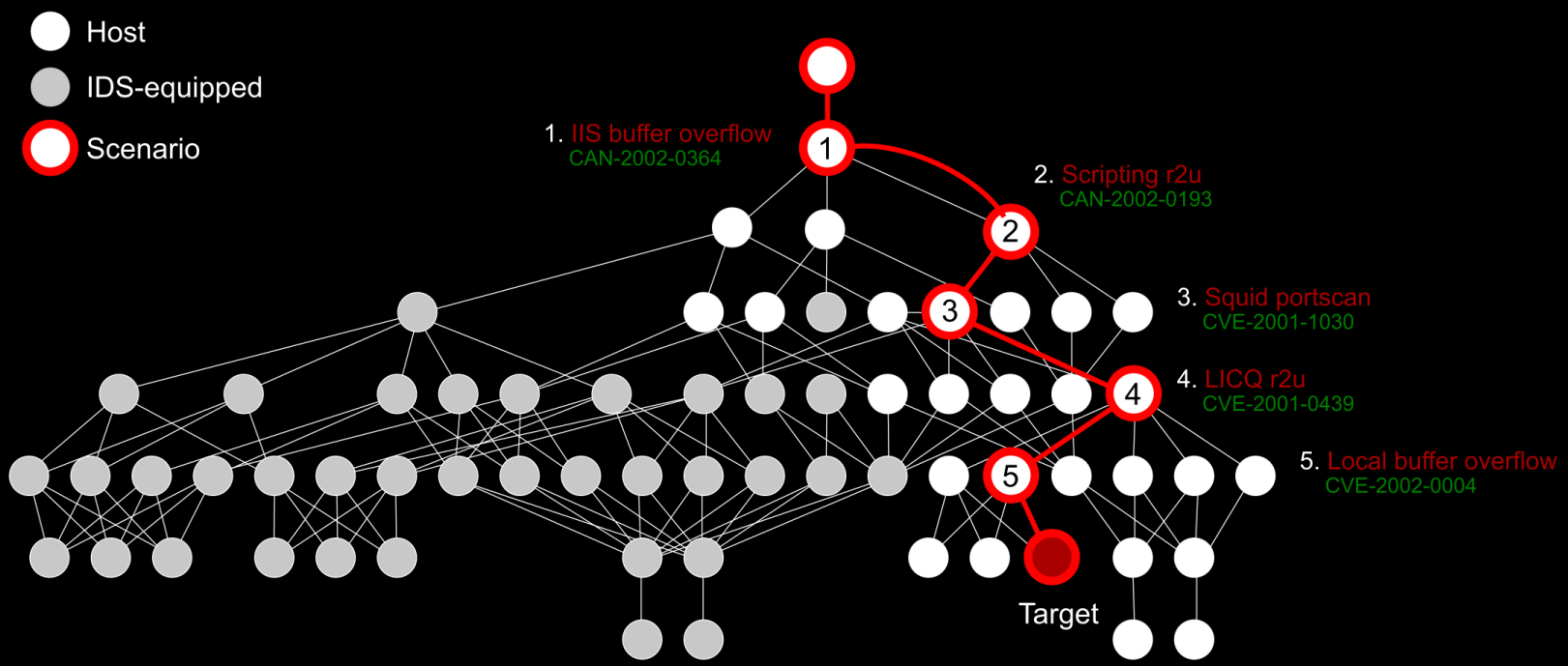
Attack graph

A more elaborate attack



Attack graph

A more elaborate attack



How hard is it? How long is it? Why aren't all hosts IDS-equipped? Can this strategy be automatically discovered?

Table of Contents

Counter-measures

Counter-measures

We know how we are going to be attacked.

Counter-measures

We know how we are going to be attacked.

It's not gonna be pretty.

Counter-measures

We know how we are going to be attacked.

It's not gonna be pretty.

Can we sabotage the attacker's plan?

Honeypots

Honeypots

Idea:

Honeypots

Idea: attackers can't resist putting their hands in honey pots.

Honeypots

Idea: attackers can't resist putting their hands in honey pots. Catch cyberterrorists red-handed!

Honeypots

Idea: attackers can't resist putting their hands in honey pots.
Catch cyberterrorists red-handed!

Honeypots

Honeypots are

Honeypots

Honeypots are

- Deliberately visible and vulnerable machines

Honeypots

Honeypots are

- Deliberately visible and vulnerable machines
- Isolated from the real infrastructure (and therefore untrusted)

Honeypots

Honeypots are

- Deliberately visible and vulnerable machines
- Isolated from the real infrastructure (and therefore untrusted)
- Giving attackers false information (software, network, ...)

Honeypots

Honeypots are

- Deliberately visible and vulnerable machines
- Isolated from the real infrastructure (and therefore untrusted)
- Giving attackers false information (software, network, ...)
- Monitored to detect scanning attempts (no legitimate use) and attacks

Honeypots

Honeypots are

- Deliberately visible and vulnerable machines
- Isolated from the real infrastructure (and therefore untrusted)
- Giving attackers false information (software, network, ...)
- Monitored to detect scanning attempts (no legitimate use) and attacks
- Trying to force the attacker to reveal information (fingerprints...)

Honeypots

Honeypots are

- Deliberately visible and vulnerable machines
- Isolated from the real infrastructure (and therefore untrusted)
- Giving attackers false information (software, network, ...)
- Monitored to detect scanning attempts (no legitimate use) and attacks
- Trying to force the attacker to reveal information (fingerprints...)
- Sometimes collaborating with others

Honeypots

Honeypots are

- Deliberately visible and vulnerable machines
- Isolated from the real infrastructure (and therefore untrusted)
- Giving attackers false information (software, network, ...)
- Monitored to detect scanning attempts (no legitimate use) and attacks
- Trying to force the attacker to reveal information (fingerprints...)
- Sometimes collaborating with others

Remember the cyber-attack maps?

What's the defence plan?

What would Sun Tsu say?

What's the defence plan?

What would Sun Tsu say?

- For each step of the attack plan

What's the defence plan?

What would Sun Tsu say?

- For each step of the attack plan
- Have the corresponding protections

What's the defence plan?

What would Sun Tsu say?

- For each step of the attack plan
- Have the corresponding protections
- Also, *when under attack*, mobilise more troops.

What's the defence plan?

What would Sun Tsu say?

- For each step of the attack plan
- Have the corresponding protections
- Also, *when under attack*, mobilise more troops.

Note: This is complementary to the (topological) defence-in-depth paradigm.

To each step, a counter-step

1. Be invisible, be unfathomable

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals.

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals.
How do they know about them? How to prevent that?

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals. How do they know about them? How to prevent that?

- Open data (maps, phonebooks...):

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals. How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals. How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media:

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals. How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media: public image management?

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals. How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media: public image management?
- Delation:

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals.
How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media: public image management?
- Delation: NDAs? least priviledge?

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals. How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media: public image management?
- Delation: NDAs? least priviledge?
- Investigation:

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals.
How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media: public image management?
- Delation: NDAs? least priviledge?
- Investigation: access control?

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals.
How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media: public image management?
- Delation: NDAs? least priviledge?
- Investigation: access control?

Problem 0:

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals.
How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media: public image management?
- Delation: NDAs? least priviledge?
- Investigation: access control?

Problem 0: information acquired is never lost.

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals.
How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media: public image management?
- Delation: NDAs? least priviledge?
- Investigation: access control?

Problem 0: information acquired is never lost.
Problem 1:

To each step, a counter-step

1. Be invisible, be unfathomable

Attackers target high (symbolic) value organisations or individuals.
How do they know about them? How to prevent that?

- Open data (maps, phonebooks...): hiding? no advertisement?
- Media: public image management?
- Delation: NDAs? least priviledge?
- Investigation: access control?

Problem 0: information acquired is never lost.
Problem 1: change is hard.

2. Be up-to-date, be tamper-proof

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...):

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...):

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...): obfuscate? tamper-proof?

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...): obfuscate? tamper-proof?
- Poking (fuzzing, scanning...):

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...): obfuscate? tamper-proof?
- Poking (fuzzing, scanning...): block? anonymise?

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...): obfuscate? tamper-proof?
- Poking (fuzzing, scanning...): block? anonymise?
- Poisoning (infiltration...):

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...): obfuscate? tamper-proof?
- Poking (fuzzing, scanning...): block? anonymise?
- Poisoning (infiltration...): audit? audit the audit?

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...): obfuscate? tamper-proof?
- Poking (fuzzing, scanning...): block? anonymise?
- Poisoning (infiltration...): audit? audit the audit?

Problem 2:

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...): obfuscate? tamper-proof?
- Poking (fuzzing, scanning...): block? anonymise?
- Poisoning (infiltration...): audit? audit the audit?

Problem 2: if you don't analyse yourself, someone else will.

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...): obfuscate? tamper-proof?
- Poking (fuzzing, scanning...): block? anonymise?
- Poisoning (infiltration...): audit? audit the audit?

Problem 2: if you don't analyse yourself, someone else will.
Tip:

2. Be up-to-date, be tamper-proof

Attackers will test the system and leverage their knowledge to find vulnerabilities.
How do they find them? How to prevent that?

- Known vulnerabilities (CVEs...): update? what about wontfixes? find them first?
- Analysis (RCE...): obfuscate? tamper-proof?
- Poking (fuzzing, scanning...): block? anonymise?
- Poisoning (infiltration...): audit? audit the audit?

Problem 2: if you don't analyse yourself, someone else will.
Tip: reduce attack surface.

3. Be unpredictable, fail silently

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found.

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found.
How to make that hard?

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found. How to make that hard?

- Don't let them control the environment:

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found. How to make that hard?

- Don't let them control the environment: introduce unknowns (randomness...)

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found. How to make that hard?

- Don't let them control the environment: introduce unknowns (randomness...)
- Reduce the window of opportunity:

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found. How to make that hard?

- Don't let them control the environment: introduce unknowns (randomness...)
- Reduce the window of opportunity: timetables...

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found. How to make that hard?

- Don't let them control the environment: introduce unknowns (randomness...)
- Reduce the window of opportunity: timetables...
- If you must fail, fail silently:

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found. How to make that hard?

- Don't let them control the environment: introduce unknowns (randomness...)
- Reduce the window of opportunity: timetables...
- If you must fail, fail silently: redundancy, no debug symbols, error messages...

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found. How to make that hard?

- Don't let them control the environment: introduce unknowns (randomness...)
- Reduce the window of opportunity: timetables...
- If you must fail, fail silently: redundancy, no debug symbols, error messages...

Problem 3:

3. Be unpredictable, fail silently

Attackers will tailor exploits for the vulnerabilities they have found. How to make that hard?

- Don't let them control the environment: introduce unknowns (randomness...)
- Reduce the window of opportunity: timetables...
- If you must fail, fail silently: redundancy, no debug symbols, error messages...

Problem 3: by design, these procedures make troubleshooting hard for you as well.

4. Think strategically, restrict priviledges

4. Think strategically, restrict priviledges

The attacker will try to abuse your systems with her weapons in order to achieve something.

4. Think strategically, restrict priviledges

The attacker will try to abuse your systems with her weapons in order to achieve something.

- Find out what she's after and... stop her? lure her? consequences?

4. Think strategically, restrict priviledges

The attacker will try to abuse your systems with her weapons in order to achieve something.

- Find out what she's after and... stop her? lure her? consequences?
- The further she gets into your system, the better you know how

4. Think strategically, restrict priviledges

The attacker will try to abuse your systems with her weapons in order to achieve something.

- Find out what she's after and... stop her? lure her? consequences?
- The further she gets into your system, the better you know how
- Restrict programs and users (PLP) – no shortcut

4. Think strategically, restrict priviledges

The attacker will try to abuse your systems with her weapons in order to achieve something.

- Find out what she's after and... stop her? lure her? consequences?
- The further she gets into your system, the better you know how
- Restrict programs and users (PLP) – no shortcut

Problem 4:

4. Think strategically, restrict priviledges

The attacker will try to abuse your systems with her weapons in order to achieve something.

- Find out what she's after and... stop her? lure her? consequences?
- The further she gets into your system, the better you know how
- Restrict programs and users (PLP) – no shortcut

Problem 4: when that happens, it's probably too late...

5. Recover and pursue

5. Recover and pursue

Attackers have succeeded, now they want to get away.

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics:

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover:

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue:

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue: share forensic evidence with investigators and judges

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue: share forensic evidence with investigators and judges

Note:

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue: share forensic evidence with investigators and judges

Note: if you're still under attack, this information might help to stop the attack.

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue: share forensic evidence with investigators and judges

Note: if you're still under attack, this information might help to stop the attack.
Problem 5:

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue: share forensic evidence with investigators and judges

Note: if you're still under attack, this information might help to stop the attack.
Problem 5: only certified professionals can acquire forensic evidence.

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue: share forensic evidence with investigators and judges

Note: if you're still under attack, this information might help to stop the attack.
Problem 5: only certified professionals can acquire forensic evidence.
Problem 6:

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue: share forensic evidence with investigators and judges

Note: if you're still under attack, this information might help to stop the attack.
Problem 5: only certified professionals can acquire forensic evidence.
Problem 6: pursuit takes time and money.

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue: share forensic evidence with investigators and judges

Note: if you're still under attack, this information might help to stop the attack.
Problem 5: only certified professionals can acquire forensic evidence.
Problem 6: pursuit takes time and money.
Problem 7:

5. Recover and pursue

Attackers have succeeded, now they want to get away.
What can you do?

- Forensics: acquire *evidence* for later analysis
- Recover: replace destroyed hardware, sanitize software, ...
- Pursue: share forensic evidence with investigators and judges

Note: if you're still under attack, this information might help to stop the attack.
Problem 5: only certified professionals can acquire forensic evidence.
Problem 6: pursuit takes time and money.
Problem 7: your chances of success in pursuit are not brilliant.

6. Forgetfulness is unforgivable

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

- Your risk analysis is incorrect

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

- Your risk analysis is incorrect
- Your protections are inadequate

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

- Your risk analysis is incorrect
- Your protections are inadequate

Accept this fact, and **update the system**.

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

- Your risk analysis is incorrect
- Your protections are inadequate

Accept this fact, and **update the system**.

Note:

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

- Your risk analysis is incorrect
- Your protections are inadequate

Accept this fact, and **update the system**.

Note: to know history, one has to *keep it* and *learn it*.

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

- Your risk analysis is incorrect
- Your protections are inadequate

Accept this fact, and **update the system**.

Note: to know history, one has to *keep it* and *learn it*.
Problem 1: (again)

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

- Your risk analysis is incorrect
- Your protections are inadequate

Accept this fact, and **update the system**.

Note: to know history, one has to *keep it* and *learn it*.
Problem 1: (again) change is hard.

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

- Your risk analysis is incorrect
- Your protections are inadequate

Accept this fact, and **update the system**.

Note: to know history, one has to *keep it* and *learn it*.
Problem 1: (again) change is hard.
Problem 8:

6. Forgetfulness is unforgivable

If your attack history does not fit your risk analysis, then:

- Your risk analysis is incorrect
- Your protections are inadequate

Accept this fact, and **update the system**.

Note: to know history, one has to *keep it* and *learn it*.
Problem 1: (again) change is hard.
Problem 8: change takes time.

Better unsafe than sorry

All this line of defence requires **careful preparation**.

More importantly, it requires that you **update quickly**.

Pipo mode: ISO 27000s Denning wheel (Plan, Do, **Check**, Act)

Ah, also, listen to your experts.

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy
2. Don't solve the wrong problem

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy
2. Don't solve the wrong problem
3. Don't sell security bottom-up

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy
2. Don't solve the wrong problem
3. Don't sell security bottom-up
4. Don't use cryptographic overkill

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy
2. Don't solve the wrong problem
3. Don't sell security bottom-up
4. Don't use cryptographic overkill
5. Don't make it complicated

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy
2. Don't solve the wrong problem
3. Don't sell security bottom-up
4. Don't use cryptographic overkill
5. Don't make it complicated
6. Don't make it expensive

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy
2. Don't solve the wrong problem
3. Don't sell security bottom-up
4. Don't use cryptographic overkill
5. Don't make it complicated
6. Don't make it expensive
7. Don't use a single line of defence

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy
2. Don't solve the wrong problem
3. Don't sell security bottom-up
4. Don't use cryptographic overkill
5. Don't make it complicated
6. Don't make it expensive
7. Don't use a single line of defence
8. Don't forget the mystery attack

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy
2. Don't solve the wrong problem
3. Don't sell security bottom-up
4. Don't use cryptographic overkill
5. Don't make it complicated
6. Don't make it expensive
7. Don't use a single line of defence
8. Don't forget the mystery attack
9. Don't trust systems

Shamir's Ten Commandments

Crypto'95, also Turing lecture 2004

1. Don't aim for perfect secrecy
2. Don't solve the wrong problem
3. Don't sell security bottom-up
4. Don't use cryptographic overkill
5. Don't make it complicated
6. Don't make it expensive
7. Don't use a single line of defence
8. Don't forget the mystery attack
9. Don't trust systems
10. Don't trust people.

Incident response

All hell loose

Situation:

Incident response

All hell loose

Situation:

- You didn't prepare correctly, and something went wrong

Incident response

All hell loose

Situation:

- You didn't prepare correctly, and something went wrong
- You prepared correctly, and something went wrong

Incident response

All hell loose

Situation:

- You didn't prepare correctly, and something went wrong
- You prepared correctly, and something went wrong
- Whatever, something's wrong

Incident response

All hell loose

Situation:

- You didn't prepare correctly, and something went wrong
- You prepared correctly, and something went wrong
- Whatever, something's wrong

Question:

Incident response

All hell loose

Situation:

- You didn't prepare correctly, and something went wrong
- You prepared correctly, and something went wrong
- Whatever, something's wrong

Question: how do you know?

Incident response

All hell loose

Situation:

- You didn't prepare correctly, and something went wrong
- You prepared correctly, and something went wrong
- Whatever, something's wrong

Question: how do you know? Detection (after the break).

Incident response

All hell loose

Situation:

- You didn't prepare correctly, and something went wrong
- You prepared correctly, and something went wrong
- Whatever, something's wrong

Question: how do you know? Detection (after the break).
Question 2:

Incident response

All hell loose

Situation:

- You didn't prepare correctly, and something went wrong
- You prepared correctly, and something went wrong
- Whatever, something's wrong

Question: how do you know? Detection (after the break).
Question 2: ok, so what do you do now?

Incident response plan

Three rules

Incident response plan

Three rules

1. **You should have an IRP ready**.

Incident response plan

Three rules

1. **You should have an IRP ready**.
2. If the IRP fits the situation, **use it**.

Incident response plan

Three rules

1. **You should have an IRP ready**.
2. If the IRP fits the situation, **use it**.
3. If the IRP doesn't fit the situation, **be insured** or you're screwed.

Incident response plan

Three rules

1. **You should have an IRP ready**.
2. If the IRP fits the situation, **use it**.
3. If the IRP doesn't fit the situation, **be insured** or you're screwed.

Hint:

Incident response plan

Three rules

1. **You should have an IRP ready**.
2. If the IRP fits the situation, **use it**.
3. If the IRP doesn't fit the situation, **be insured** or you're screwed.

Hint: prepare *before* incidents happen.

Incident response plan

Three actors

1. **Management**:

Incident response plan

Three actors

1. **Management**: want things work, want no responsibility, want give blame

Incident response plan

Three actors

1. **Management**: want things work, want no responsibility, want give blame
2. **Law officers**:

Incident response plan

Three actors

1. **Management**: want things work, want no responsibility, want give blame
2. **Law officers**: want catch bad guys, want evidence, want law respected

Incident response plan

Three actors

1. **Management**: want things work, want no responsibility, want give blame
2. **Law officers**: want catch bad guys, want evidence, want law respected
3. **IT team**:

Incident response plan

Three actors

1. **Management**: want things work, want no responsibility, want give blame
2. **Law officers**: want catch bad guys, want evidence, want law respected
3. **IT team**: want cut power, want stop hacker, want understand things

Incident response plan

Three actors

1. **Management**: want things work, want no responsibility, want give blame
2. **Law officers**: want catch bad guys, want evidence, want law respected
3. **IT team**: want cut power, want stop hacker, want understand things

Hint:

Incident response plan

Three actors

1. **Management**: want things work, want no responsibility, want give blame
2. **Law officers**: want catch bad guys, want evidence, want law respected
3. **IT team**: want cut power, want stop hacker, want understand things

Hint: put them together in a room.

Incident response plan

Three actors

1. **Management**: want things work, want no responsibility, want give blame
2. **Law officers**: want catch bad guys, want evidence, want law respected
3. **IT team**: want cut power, want stop hacker, want understand things

Hint: put them together in a room.
Hint 2:

Incident response plan

Three actors

1. **Management**: want things work, want no responsibility, want give blame
2. **Law officers**: want catch bad guys, want evidence, want law respected
3. **IT team**: want cut power, want stop hacker, want understand things

Hint: put them together in a room.
Hint 2: management takes the blame for things agreed upon, you take the blame if you deviate from the plan.

Incident response plan

Three key points

Incident response plan

Three key points

1. Decide who to contact and gather in case of incident (response team), their role and **responsibilities**

Incident response plan

Three key points

1. Decide who to contact and gather in case of incident (response team), their role and **responsibilities**
2. Decide what **priorities** are and set bounds to what is acceptable

Incident response plan

Three key points

1. Decide who to contact and gather in case of incident (response team), their role and **responsibilities**
2. Decide what **priorities** are and set bounds to what is acceptable
3. Decide what operations to undertake, check that they work as intended, and **debrief**

Incident response plan

Three key points

1. Decide who to contact and gather in case of incident (response team), their role and **responsibilities**
2. Decide what **priorities** are and set bounds to what is acceptable
3. Decide what operations to undertake, check that they work as intended, and **debrief**

Hint:

Incident response plan

Three key points

1. Decide who to contact and gather in case of incident (response team), their role and **responsibilities**
2. Decide what **priorities** are and set bounds to what is acceptable
3. Decide what operations to undertake, check that they work as intended, and **debrief**

Hint: In the workplace, your responsibility is often to act as determined by the hierarchy. Just make sure they write it down.

Stuxnet?