OSY.SSI[2015][A]

Detection, Surveillance

Bonus: Video

Detection and Surveillance

What for?

Fact:

Detection and Surveillance

What for?

Fact: optimal security efforts are adapted to context.

Detection and Surveillance

What for?

Fact: optimal security efforts are adapted to context.
Hint:

Detection and Surveillance

What for?

Fact: optimal security efforts are adapted to context.
Hint: be (context-)aware.

Detection and Surveillance

What for?

Fact: optimal security efforts are adapted to context.
Hint: be (context-)aware.

Fact:

Detection and Surveillance

What for?

Fact: optimal security efforts are adapted to context.
Hint: be (context-)aware.

Fact: context may change.

Detection and Surveillance

What for?

Fact: optimal security efforts are adapted to context.
Hint: be (context-)aware.

Fact: context may change.
Hint:

Detection and Surveillance

What for?

Fact: optimal security efforts are adapted to context.
Hint: be (context-)aware.

Fact: context may change.
Hint: be reactive, be proactive.

Detection and Surveillance

What for?

Fact: optimal security efforts are adapted to context.
Hint: be (context-)aware.

Fact: context may change.
Hint: be reactive, be proactive.

Table of Contents

Preliminary: On statistics
- Binary classifiers
- Bayes' theorem

Detection theory
- Blind source separation
- Some examples

Improving detection

Detection

A detector monitors a certain phenomenon and outputs a result.

Detection

A detector monitors a certain phenomenon and outputs a result.
For simplicity, assume that the result is 0 or 1.

Detection

A detector monitors a certain phenomenon and outputs a result. For simplicity, assume that the result is 0 or 1.

Detection is relevant if the result is correct.

Detection

A detector monitors a certain phenomenon and outputs a result.
For simplicity, assume that the result is 0 or 1.

Detection is relevant if the result is correct.
Confusion matrix:

Detection

A detector monitors a certain phenomenon and outputs a result.
For simplicity, assume that the result is 0 or 1.

Detection is relevant if the result is correct.
Confusion matrix:

	Danger	No danger
1	True positive	False positive
0	False negative	True negative

Confusion matrix

Type II and type I error rates

Confusion matrix

Type II and type I error rates

Sensitivity

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Specificity

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Specificity (exclude a condition correctly, i.e. no innocent in prison):

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Specificity (exclude a condition correctly, i.e. no innocent in prison):

$$SPC = \frac{TN}{FP + TN}$$

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Specificity (exclude a condition correctly, i.e. no innocent in prison):

$$SPC = \frac{TN}{FP + TN}$$

A perfect predictor would be 100% sensitive and 100% specific.

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Specificity (exclude a condition correctly, i.e. no innocent in prison):

$$SPC = \frac{TN}{FP + TN}$$

A perfect predictor would be 100% sensitive and 100% specific.
Fact:

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Specificity (exclude a condition correctly, i.e. no innocent in prison):

$$SPC = \frac{TN}{FP + TN}$$

A perfect predictor would be 100% sensitive and 100% specific.
Fact: mathematically impossible.

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Specificity (exclude a condition correctly, i.e. no innocent in prison):

$$SPC = \frac{TN}{FP + TN}$$

A perfect predictor would be 100% sensitive and 100% specific.
Fact: mathematically impossible.
Consequence:

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Specificity (exclude a condition correctly, i.e. no innocent in prison):

$$SPC = \frac{TN}{FP + TN}$$

A perfect predictor would be 100% sensitive and 100% specific.
Fact: mathematically impossible.
Consequence: For any test, there is usually a trade-off between the measures – *e.g.* ROC.

Confusion matrix

Type II and type I error rates

Sensitivity (identify a condition correctly, i.e. no loose criminal):

$$TPR = \frac{TP}{TP + FN}$$

Specificity (exclude a condition correctly, i.e. no innocent in prison):

$$SPC = \frac{TN}{FP + TN}$$

A perfect predictor would be 100% sensitive and 100% specific.
Fact: mathematically impossible.
Consequence: For any test, there is usually a trade-off between the measures – *e.g.* ROC.

Bayes' theorem

Theorem (Bayes, 1763)

Bayes' theorem

Theorem (Bayes, 1763)

$A, B, \mathbb{P}(B) > 0,$

$$\mathbb{P}(A|B) = \frac{\mathbb{P}(B|A)\mathbb{P}(A)}{\mathbb{P}(B)}$$

Bayes' theorem

Application: catching criminals

Hypotheses:

Bayes' theorem

Application: catching criminals

Hypotheses:

- if X is criminal, D returns 1 with probability 99%

Bayes' theorem

Application: catching criminals

Hypotheses:

- if X is criminal, D returns 1 with probability 99%
- if X is innocent, D returns 0 with probability 99%

Bayes' theorem

Application: catching criminals

Hypotheses:

- if X is criminal, D returns 1 with probability 99%
- if X is innocent, D returns 0 with probability 99%
- One person in 10,000 is a criminal

Bayes' theorem

Application: catching criminals

Hypotheses:

- if X is criminal, D returns 1 with probability 99%
- if X is innocent, D returns 0 with probability 99%
- One person in 10,000 is a criminal

Question :

Bayes' theorem

Application: catching criminals

Hypotheses:

- if X is criminal, D returns 1 with probability 99%
- if X is innocent, D returns 0 with probability 99%
- One person in 10,000 is a criminal

Question : $D(X) = 1$, what is the probability that X is criminal ?

Bayes' theorem

Application: catching criminals

Hypotheses:

- if X is criminal, D returns 1 with probability 99%
- if X is innocent, D returns 0 with probability 99%
- One person in 10,000 is a criminal

Question : $D(X) = 1$, what is the probability that X is criminal ?

Bayes' theorem

Application: catching criminals

$$\begin{aligned}
\mathbb{P}(X \text{ criminal} | D = 1) &= \mathbb{P}(D = 1 | X \text{ criminal}) \frac{\mathbb{P}(X \text{ criminal})}{\mathbb{P}(D = 1)} \\
&= 0.99 \frac{1/10^4}{0.99 \times 10^{-4} + 0.01 \times (1 - 10^{-4})} \\
&\approx 0.01
\end{aligned}$$

Bayes' theorem

Application: catching criminals

$$\begin{aligned}\mathbb{P}(X \text{ criminal}|D=1) &= \mathbb{P}(D=1|X \text{ criminal})\frac{\mathbb{P}(X \text{ criminal})}{\mathbb{P}(D=1)} \\ &= 0.99\frac{1/10^4}{0.99\times 10^{-4}+0.01\times(1-10^{-4})} \\ &\approx 0.01\end{aligned}$$

Consequence: there is a 99% chance that X is innocent...

Bayes' theorem

Application: catching criminals

$$\begin{aligned}\mathbb{P}(X \text{ criminal}|D=1) &= \mathbb{P}(D=1|X \text{ criminal})\frac{\mathbb{P}(X \text{ criminal})}{\mathbb{P}(D=1)} \\ &= 0.99\frac{1/10^4}{0.99\times 10^{-4}+0.01\times(1-10^{-4})} \\ &\approx 0.01\end{aligned}$$

Consequence: there is a 99% chance that X is innocent...
Remark:

Bayes' theorem

Application: catching criminals

$$\begin{aligned}\mathbb{P}(X \text{ criminal}|D=1) &= \mathbb{P}(D=1|X \text{ criminal})\frac{\mathbb{P}(X \text{ criminal})}{\mathbb{P}(D=1)} \\ &= 0.99\frac{1/10^4}{0.99\times 10^{-4}+0.01\times(1-10^{-4})} \\ &\approx 0.01\end{aligned}$$

Consequence: there is a 99% chance that X is innocent...
Remark: in reality, tests are not that accurate, and there are not that many criminals.

Note: This is one of the reasons why unwarranted search is illegal and invalid in a court of justice.

Bayes' theorem

There's no free meal

Facts

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**
- Even assuming random sampling, **rare events are hard to detect**

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**
- Even assuming random sampling, **rare events are hard to detect**
- Random sampling **is a wrong hypothesis**.

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**
- Even assuming random sampling, **rare events are hard to detect**
- Random sampling **is a wrong hypothesis**.
- For every criminal you catch this way, **many innocents are condemned**.

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**
- Even assuming random sampling, **rare events are hard to detect**
- Random sampling **is a wrong hypothesis**.
- For every criminal you catch this way, **many innocents are condemned**.
- **Everyone** gets slowed down.

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**
- Even assuming random sampling, **rare events are hard to detect**
- Random sampling **is a wrong hypothesis**.
- For every criminal you catch this way, **many innocents are condemned**.
- **Everyone** gets slowed down.

Consequence:

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**
- Even assuming random sampling, **rare events are hard to detect**
- Random sampling **is a wrong hypothesis**.
- For every criminal you catch this way, **many innocents are condemned**.
- **Everyone** gets slowed down.

Consequence: dragnet surveillance is not only useless, it is dangerous.

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**
- Even assuming random sampling, **rare events are hard to detect**
- Random sampling **is a wrong hypothesis**.
- For every criminal you catch this way, **many innocents are condemned**.
- **Everyone** gets slowed down.

Consequence: dragnet surveillance is not only useless, it is dangerous.
Consequence 2:

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**
- Even assuming random sampling, **rare events are hard to detect**
- Random sampling **is a wrong hypothesis**.
- For every criminal you catch this way, **many innocents are condemned**.
- **Everyone** gets slowed down.

Consequence: dragnet surveillance is not only useless, it is dangerous.
Consequence 2: intrusion detection is hard.

Bayes' theorem

There's no free meal

Facts

- Most detections are **false positives**
- Even assuming random sampling, **rare events are hard to detect**
- Random sampling **is a wrong hypothesis**.
- For every criminal you catch this way, **many innocents are condemned**.
- **Everyone** gets slowed down.

Consequence: dragnet surveillance is not only useless, it is dangerous.
Consequence 2: intrusion detection is hard.

Table of Contents

Preliminary: On statistics
- Binary classifiers
- Bayes' theorem

Detection theory
- Blind source separation
- Some examples

Improving detection

What is a detector?

A detector is really a *statistical test* in disguise.

What is a detector?

A detector is really a *statistical test* in disguise.

Implicitly, it tries to determine whether a given input X belongs to distribution H_0 (correct input) or not (malicious input).

What is a detector?

A detector is really a *statistical test* in disguise.

Implicitly, it tries to determine whether a given input X belongs to distribution H_0 (correct input) or not (malicious input).

Examples:

What is a detector?

A detector is really a *statistical test* in disguise.

Implicitly, it tries to determine whether a given input X belongs to distribution H_0 (correct input) or not (malicious input).

Examples:

- X never happens in H_0, so if X, then alarm (trigger)

What is a detector?

A detector is really a *statistical test* in disguise.

Implicitly, it tries to determine whether a given input X belongs to distribution H_0 (correct input) or not (malicious input).

Examples:

- X never happens in H_0, so if X, then alarm (trigger)
- X never happens alone in H_0 (conjunction)

What is a detector?

A detector is really a *statistical test* in disguise.

Implicitly, it tries to determine whether a given input X belongs to distribution H_0 (correct input) or not (malicious input).

Examples:

- X never happens in H_0, so if X, then alarm (trigger)
- X never happens alone in H_0 (conjunction)
- X appears rarely in H_0 (hypothesis testing)

What is a detector?

A detector is really a *statistical test* in disguise.

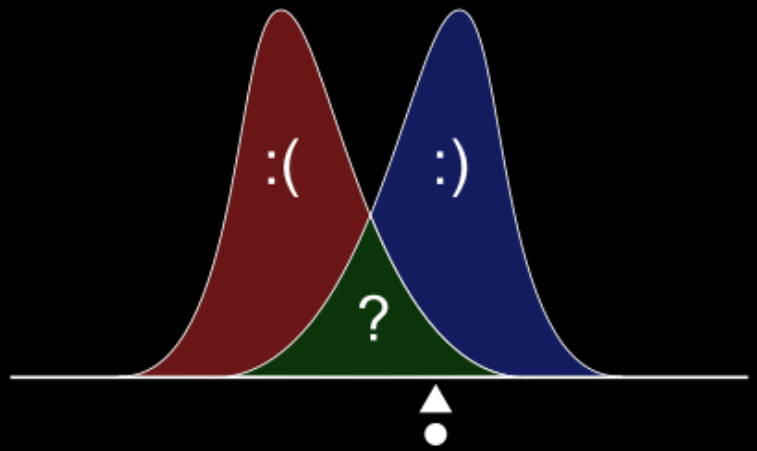
Implicitly, it tries to determine whether a given input X belongs to distribution H_0 (correct input) or not (malicious input).

Examples:

- X never happens in H_0, so if X, then alarm (trigger)
- X never happens alone in H_0 (conjunction)
- X appears rarely in H_0 (hypothesis testing)
- etc.

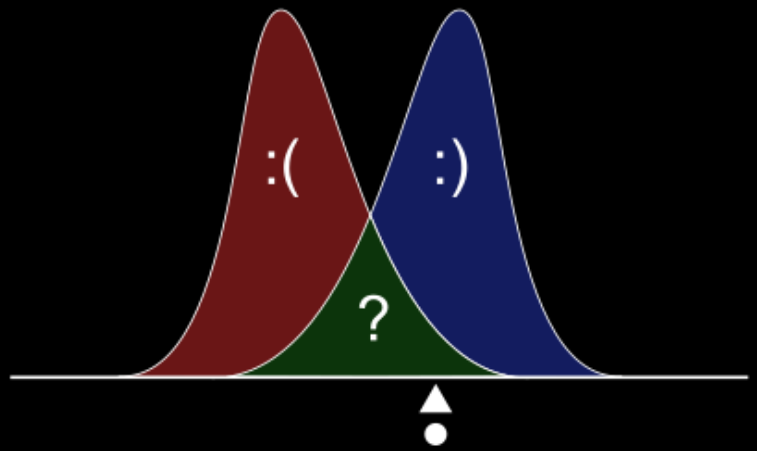
What is a detector?

Illustration



What is a detector?

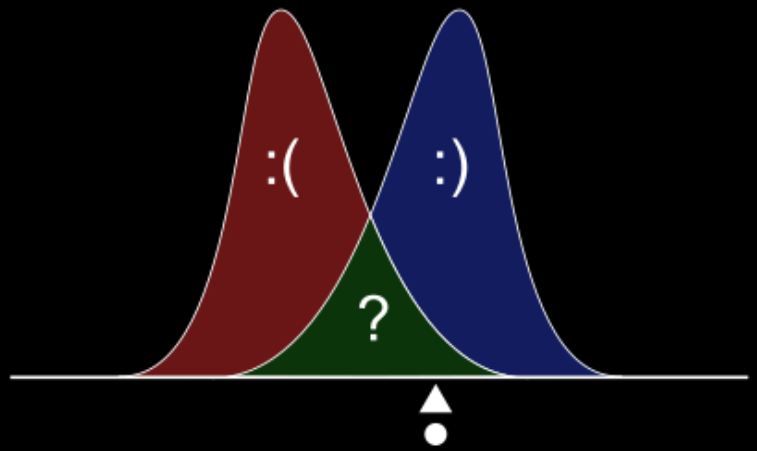
Illustration



Examples:

What is a detector?

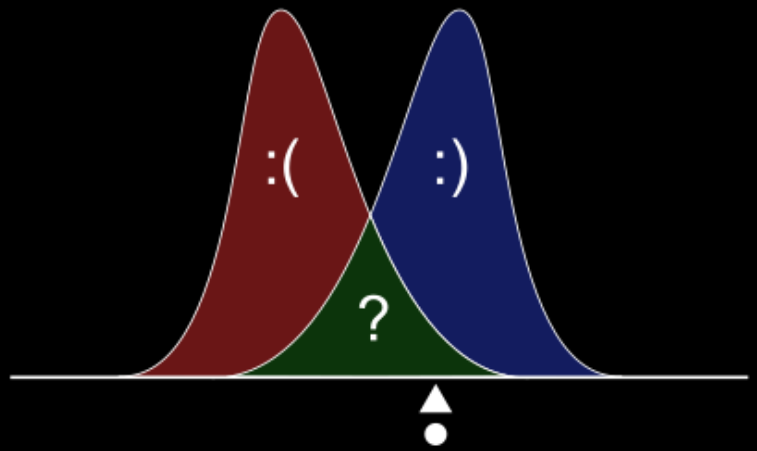
Illustration



Examples: signatures, protocol usage, heuristics, machine learning...

What is a detector?

Illustration

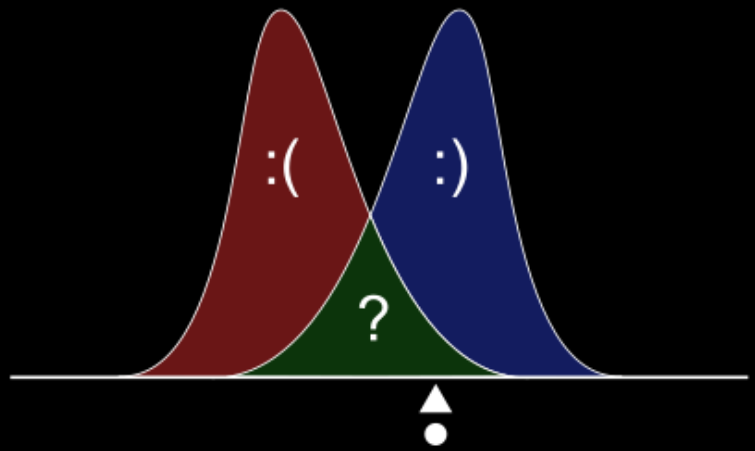


Examples: signatures, protocol usage, heuristics, machine learning...

Note:

What is a detector?

Illustration



Examples: signatures, protocol usage, heuristics, machine learning...

Note: usually, distributions aren't really known nor static

Data mining

Problem:

Data mining

Problem: one detector is unreliable.

Data mining

Problem: one detector is unreliable.
Solution:

Data mining

Problem: one detector is unreliable.
Solution: put many detectors!

Data mining

Problem: one detector is unreliable.
Solution: put many detectors!
Problem:

Data mining

Problem: one detector is unreliable.
Solution: put many detectors!
Problem: Wow. Such data! Much false alarm.

Data mining

Problem: one detector is unreliable.
Solution: put many detectors!
Problem: Wow. Such data! Much false alarm.
Solution:

Data mining

Problem: one detector is unreliable.
Solution: put many detectors!
Problem: Wow. Such data! Much false alarm.
Solution: data mining/machine learning (e.g. Bayesian networks)!

Data mining

Problem: one detector is unreliable.
Solution: put many detectors!
Problem: Wow. Such data! Much false alarm.
Solution: data mining/machine learning (e.g. Bayesian networks)!

Remark:

Data mining

Problem: one detector is unreliable.
Solution: put many detectors!
Problem: Wow. Such data! Much false alarm.
Solution: data mining/machine learning (e.g. Bayesian networks)!

Remark: ML may tell you that something is wrong, but what?
and what to do?

Data mining

Problem: one detector is unreliable.
Solution: put many detectors!
Problem: Wow. Such data! Much false alarm.
Solution: data mining/machine learning (e.g. Bayesian networks)!

Remark: ML may tell you that something is wrong, but what?
and what to do?

The Nanny's Solution

Causality, symptoms and psychopaths

The Nanny's Solution

Causality, symptoms and psychopaths

- A child cries

The Nanny's Solution

Causality, symptoms and psychopaths

- A child cries
- The nanny comes

The Nanny's Solution

Causality, symptoms and psychopaths

- A child cries
- The nanny comes
- The nanny shakes the baby very hard

The Nanny's Solution

Causality, symptoms and psychopaths

- A child cries
- The nanny comes
- The nanny shakes the baby very hard
- The child does not cry anymore

The Nanny's Solution

Causality, symptoms and psychopaths

- A child cries
- The nanny comes
- The nanny shakes the baby very hard
- The child does not cry anymore

Question:

The Nanny's Solution

Causality, symptoms and psychopaths

- A child cries
- The nanny comes
- The nanny shakes the baby very hard
- The child does not cry anymore

Question: has the nanny solved the issue ?

The Nanny's Solution

Causality, symptoms and psychopaths

- A child cries
- The nanny comes
- The nanny shakes the baby very hard
- The child does not cry anymore

Question: has the nanny solved the issue ?

Question 2:

The Nanny's Solution

Causality, symptoms and psychopaths

- A child cries
- The nanny comes
- The nanny shakes the baby very hard
- The child does not cry anymore

Question: has the nanny solved the issue ?

Question 2: what has the nanny solved ?

The SSL warning page

Bad design, bad design, and evil users

The SSL warning page

Bad design, bad design, and evil users

- Is the connection to `ecp.fr` secured by SSL?

The SSL warning page

Bad design, bad design, and evil users

- Is the connection to `ecp.fr` secured by SSL?
- What about `tf1.fr` ?

The SSL warning page

Bad design, bad design, and evil users

- Is the connection to `ecp.fr` secured by SSL?
- What about `tf1.fr` ?
- Any warning? What's the **default situation**?

The SSL warning page

Bad design, bad design, and evil users

- Is the connection to `ecp.fr` secured by SSL?
- What about `tf1.fr` ?
- Any warning? What's the **default situation**?
- When you bypass the SSL warning, do you ever get back to secure SSL?

The SSL warning page

Bad design, bad design, and evil users

- Is the connection to `ecp.fr` secured by SSL?
- What about `tf1.fr` ?
- Any warning? What's the **default situation**?
- When you bypass the SSL warning, do you ever get back to secure SSL?

Question:

The SSL warning page

Bad design, bad design, and evil users

- Is the connection to `ecp.fr` secured by SSL?
- What about `tf1.fr` ?
- Any warning? What's the **default situation**?
- When you bypass the SSL warning, do you ever get back to secure SSL?

Question: what's the point?

The SSL warning page

Bad design, bad design, and evil users

- Is the connection to `ecp.fr` secured by SSL?
- What about `tf1.fr` ?
- Any warning? What's the **default situation**?
- When you bypass the SSL warning, do you ever get back to secure SSL?

Question: what's the point?

Also, Lenovo SuperFish.

Table of Contents

Preliminary: On statistics
- Binary classifiers
- Bayes' theorem

Detection theory
- Blind source separation
- Some examples

Improving detection

Some statistics about detection

Some statistics about detection

- 71% of victims do not realise intrusion (Trustware Global, 2014)

Some statistics about detection

- 71% of victims do not realise intrusion (Trustware Global, 2014)
- 87 days: median duration of intrusion (Symantec, 2014)

Some statistics about detection

- 71% of victims do not realise intrusion (Trustware Global, 2014)
- 87 days: median duration of intrusion (Symantec, 2014)
- Half of intrusions can be blamed on insiders (idem)

Some statistics about detection

- 71% of victims do not realise intrusion (Trustware Global, 2014)
- 87 days: median duration of intrusion (Symantec, 2014)
- Half of intrusions can be blamed on insiders (idem)

Success stories: Equation Group (14 years undetected), Windows (17 years), Gemalto ($\sim$10 years).

Different complementary approaches

Different complementary approaches

- Known-target detection (ok if not simple functionality)

Different complementary approaches

- Known-target detection (ok if not simple functionality)
- Known-attack detection (ok if small attack surface)

Different complementary approaches

- Known-target detection (ok if not simple functionality)
- Known-attack detection (ok if small attack surface)
- Honeypot early alarm (improves true detection rate)

Different complementary approaches

- Known-target detection (ok if not simple functionality)
- Known-attack detection (ok if small attack surface)
- Honeypot early alarm (improves true detection rate)
- Auditing (improves governance)

Different complementary approaches

- Known-target detection (ok if not simple functionality)
- Known-attack detection (ok if small attack surface)
- Honeypot early alarm (improves true detection rate)
- Auditing (improves governance)
- Pentesting/Red Teams (unsound but useful)

Different complementary approaches

- Known-target detection (ok if not simple functionality)
- Known-attack detection (ok if small attack surface)
- Honeypot early alarm (improves true detection rate)
- Auditing (improves governance)
- Pentesting/Red Teams (unsound but useful)
- Drills (measures performance)

Different complementary approaches

- Known-target detection (ok if not simple functionality)
- Known-attack detection (ok if small attack surface)
- Honeypot early alarm (improves true detection rate)
- Auditing (improves governance)
- Pentesting/Red Teams (unsound but useful)
- Drills (measures performance)
- Randomized in-depth testing (- specificity, + sensitivity)

Different complementary approaches

- Known-target detection (ok if not simple functionality)
- Known-attack detection (ok if small attack surface)
- Honeypot early alarm (improves true detection rate)
- Auditing (improves governance)
- Pentesting/Red Teams (unsound but useful)
- Drills (measures performance)
- Randomized in-depth testing (- specificity, + sensitivity)

The enemies of detection

The enemies of detection

- Large attack surface (always a bad idea anyway)

The enemies of detection

- Large attack surface (always a bad idea anyway)
- Moving target (but defence...)

The enemies of detection

- Large attack surface (always a bad idea anyway)
- Moving target (but defence...)
- Performance (but customers...)

The enemies of detection

- Large attack surface (always a bad idea anyway)
- Moving target (but defence...)
- Performance (but customers...)
- Incorrect threat landscape and risk estimation

The enemies of detection

- Large attack surface (always a bad idea anyway)
- Moving target (but defence...)
- Performance (but customers...)
- Incorrect threat landscape and risk estimation
- Insiders (but business...)

The enemies of detection

- Large attack surface (always a bad idea anyway)
- Moving target (but defence...)
- Performance (but customers...)
- Incorrect threat landscape and risk estimation
- Insiders (but business...)
- Not replacing failing detectors (but is it really failing?)

The enemies of detection

- Large attack surface (always a bad idea anyway)
- Moving target (but defence...)
- Performance (but customers...)
- Incorrect threat landscape and risk estimation
- Insiders (but business...)
- Not replacing failing detectors (but is it really failing?)
- Single line of defence (always a bad idea)

The enemies of detection

- Large attack surface (always a bad idea anyway)
- Moving target (but defence...)
- Performance (but customers...)
- Incorrect threat landscape and risk estimation
- Insiders (but business...)
- Not replacing failing detectors (but is it really failing?)
- Single line of defence (always a bad idea)

There is no silver bullet.

Should we vaccinate?

Fact:

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.
Fact 2:

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.
Fact 2: not using detection is **much worse**.

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.
Fact 2: not using detection is **much worse**.
Fact 3:

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.
Fact 2: not using detection is **much worse**.
Fact 3: all your risk analysis is pointless and baseless if not confronted to fact.

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.
Fact 2: not using detection is **much worse**.
Fact 3: all your risk analysis is pointless and baseless if not confronted to fact.
Fact 4:

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.
Fact 2: not using detection is **much worse**.
Fact 3: all your risk analysis is pointless and baseless if not confronted to fact.
Fact 4: not implementing proper detection is not forgivable and legally punishable.

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.
Fact 2: not using detection is **much worse**.
Fact 3: all your risk analysis is pointless and baseless if not confronted to fact.
Fact 4: not implementing proper detection is not forgivable and legally punishable.
Fact 5:

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.
Fact 2: not using detection is **much worse**.
Fact 3: all your risk analysis is pointless and baseless if not confronted to fact.
Fact 4: not implementing proper detection is not forgivable and legally punishable.
Fact 5: your undetected intrusion may, and will, propagate to others.

Should we vaccinate?

Fact: detection is expensive and high-maintenance, also has side effects.
Fact 2: not using detection is **much worse**.
Fact 3: all your risk analysis is pointless and baseless if not confronted to fact.
Fact 4: not implementing proper detection is not forgivable and legally punishable.
Fact 5: your undetected intrusion may, and will, propagate to others.

Conclusion: Use protection and vaccinate your stuff. Those telling you otherwise are dangerous.

Next time

Prepare your computers, learn/remember HTML, SQL, XML, javascript basics.

See y'all next time!