COSC130:

Topic 8: Risk Management

Lecture 8 Part 1

Uday Tupakula
A/Prof in Cyber Security
School of Science and Technology
Faculty of Science, Agriculture, Business and Law
University of New England

Overview

- Software Trends and Security Risks
- Risk Management for Software Security
- Best Practices for Software Security
- Knowledge for Software Security
- Adopting Best Practices

RISK

- **NIST:** Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
  - (i) the adverse impacts that would arise if the circumstance or event occurs
  - (ii) the likelihood of occurrence

Software Trends and Security Risks

- All aspects of modern society increasingly dependent on software systems
- Defence, Business, Finance, Energy, Transportation, Communication and Education
- Consequences of failure can be severe
- Dependable functionality and security are essential
- Trinity of trouble: connectedness, complexity and extensibility

Software Trends and Security Risks

- No silver bullet for security
- Unfortunately security continues to be sold as a product
- Most defensive mechanisms in the market do little to address the heart of the problem
- Most of them operate in reactive mode

technology

Drivers urged to update Jeep software after hackers force car off the road

This story was published: 2 HOURS AGO | JULY 22, 2015 10:50AM

I hacked a ... white-hat hackers have demonstrated that it is possible to hack a connected car and force it off the highway. *Source: Supplied*

SECURITY and motoring experts have warned drivers of the Jeep Cherokee to install a software update after hackers used a flaw in a car's infotainment system to force it off the road.

Wired has published a story by Andy Greenberg which details how white-hat hackers were able to demonstrate and expose a flaw in a car's infotainment system to take control of the vehicle while it was driving on the highway at 100km/h.

https://www.bbc.com/news/technology-33650491

Fiat Chrysler has issued a safety recall affecting 1.4m vehicles in the US, after security researchers showed that one of its cars could be hacked.

On Tuesday, tech magazine Wired **reported that hackers had taken control of a Jeep Cherokee** via its internet-connected entertainment system.

Chrysler said it was issuing a voluntary recall to update the software in affected vehicles.

The company added that hacking its vehicles was a "criminal action".

Security researchers Charlie Miller and Chris Valasek demonstrated that it was possible for hackers to control a Jeep Cherokee remotely, using the car's entertainment system which connected to the mobile data network.

The two security researchers have spent years investigating car control systems and developing ways to subvert them. The pair are due to reveal more information about their work at the Def Con hacker conference next month.

https://www.popsci.com/software-rising-cause-car-recalls/

CARS

Software Now To Blame For 15 Percent Of Car Recalls

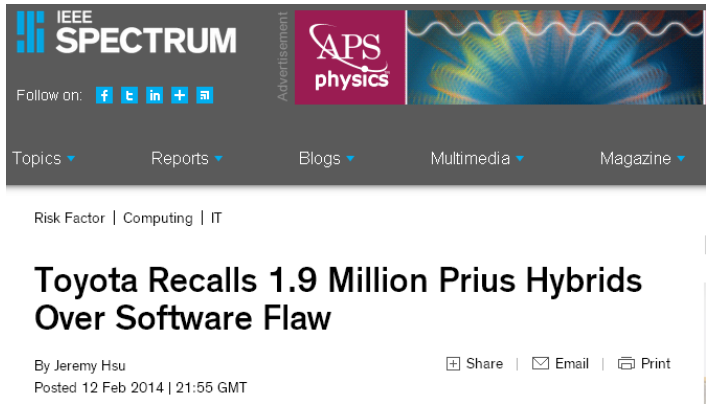
You can't just hold the home and lock buttons to solve this one

Apps freezing or crashing, unexpected sluggishness, and sudden reboots are all, unfortunately, within the normal range of behavior of the software in our smartphones and laptops.

While losing that text message you were composing might be a crisis for the moment, it's nothing compared to the catastrophe that could result from software in our cars not playing nice.

Yes, we're talking about nightmares like doors flying open without warning, or a sudden complete shutdown on the highway.

The number of software-related issues, according to several sources tracking vehicle recalls, has been on the rise. According to financial advisors Stout Risius Ross (SSR), in their Automotive Warranty & Recall Report 2016, software-related recalls have gone from less than 5 percent of recalls in 2011 to 15 percent by the end of 2015.



www.bbc.com › news › technology-44224794

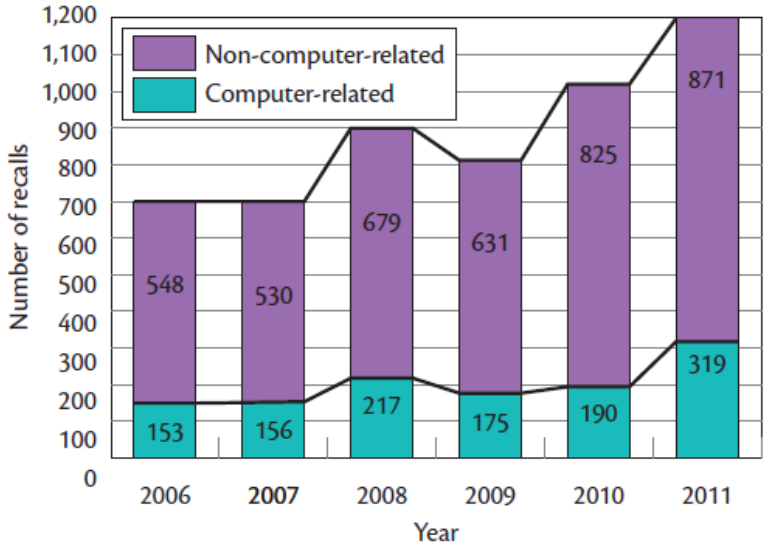
BMW cars found to contain more than a dozen flaws - BBC News

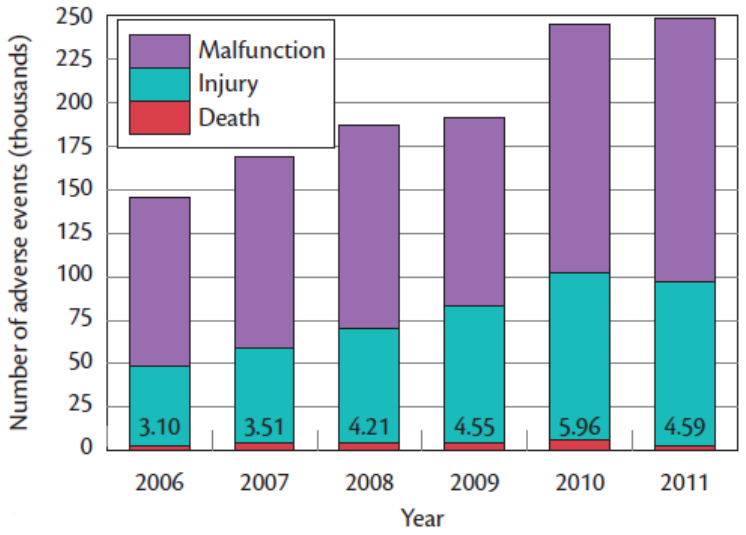
May 23, 2018 - BMW **cars** found to contain more than a dozen **flaws** ... separate **flaws**, according to a study by a Chinese cyber-**security** lab. ... Its customers have been advised to keep an eye out for **software** ... BMW advert 'promoted dangerous driving' · BMW **recalls** 300,000 **cars** over stalling risk · Could a hacker hijack ...

Failures in Medical Devices

- Malfunctioning medical devices one of the leading causes of serious injury & deaths
- Almost 23 % percent of these recalls were due to computer-related failures, of which approximately 94% medium to high risk (such as serious injury or death) of severe health consequences to patients

Source: Homa Alemzadeh, “Analysis of Safety-Critical computer failures in medical devices”, IEEE Security & Privacy, July/Aug 2013





www.fda.gov › medical-devices › safety-communications › urgent11-...

URGENT/11 Cybersecurity Vulnerabilities in a Widely ... - FDA

Oct 1, 2019 - These vulnerabilities exist in IPnet, a third-party software component that ... Security researchers, medical device manufacturers, and the FDA ...

threatpost.com › Web Security

FDA: Software Failures Responsible for 24% Of All Medical ...

Jun 20, 2012 - Software failures were behind 24 percent of all the medical device recalls in 2011, according to data from the U.S. Food and Drug ... devices by a team of researchers identified software security vulnerabilities in software that ...

www.cnbc.com › 2019/10/01 › fda-issues-warning-on-medical-device...

FDA issues warning on medical devices that are vulnerable to ...

Oct 1, 2019 - Medical devices that use third-party, decades-old software called IPnet are ... serious cybersecurity flaws in some medical devices that could allow hackers ... obtain a better understanding" of the security risk and identify medical devices ... In June, medical device maker Medtronic recalled some models of ...

www.tga.gov.au › sites › default › files › medical-device-cyber-securi... PDF

Medical device cyber security guidance for industry - TGA

Software as a Medical Device (SaMD); this includes devices that incorporate ... Is there risk that a cyber security vulnerability may lead to the ... required in response to the changed medical device cyber security risk profile, i.e. a device recall,.

karmaimpact.com › Healthcare › BioTech

FDA Warns Medical Devices May Be Vulnerable to Hackers ...

Oct 2, 2019 - Concerns about the security of medical devices date to at least 2011, when a ... recall of 465,000 pacemakers because of security vulnerabilities. ... on building their own software technologies under FDA draft guidelines, ...

www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html

Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era

By Jordan Robertson and Michael Riley | Dec 10, 2014 9:00 PM ET | **35 Comments** **Email** **Print**

The pipeline was outfitted with sensors and cameras to monitor every step of its 1,099 miles from the **Caspian Sea** to the Mediterranean. The blast that blew it out of commission didn't trigger a single distress signal.

That was bewildering, as was the cameras' failure to capture the combustion in eastern **Turkey**. But investigators shared their findings within a tight circle. The Turkish government publicly blamed a malfunction, Kurdish separatists claimed credit and **BP Plc (BP/)** had the line running again in three weeks. The explosion that lit up the night sky over Refahiye, a town known for its honey farms, seemed to be forgotten.

Photographer: Anatolian-Muhammet Ispirli/Corbis

Firemen struggle to extinguish the blaze at the Baku-Tbilisi-Ceyhan (BTC) pipeline near... **Read More**

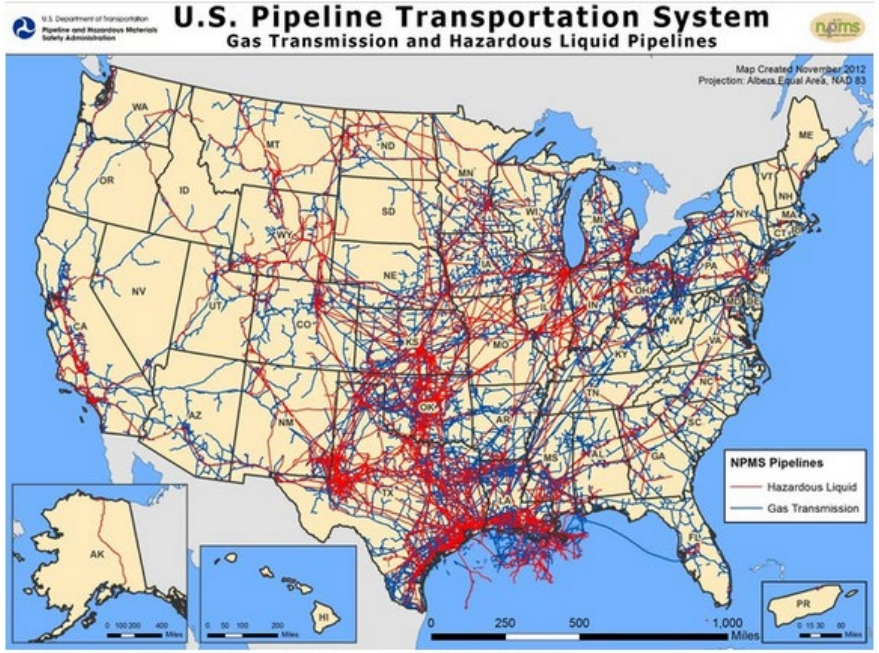
It wasn't. For western intelligence agencies, the blowout was a watershed event. Hackers had shut down alarms, cut off communications and super-pressurized the crude oil in the line, according to four people familiar with the incident who asked not to be identified because details of the investigation are confidential. The main weapon at valve station 30 on Aug. 5, 2008, was a keyboard.

Related

Map of BTC-pipeline blast

Source: Bloomberg research

Bloomberg Graphics



Source: USDOT Pipeline and Hazardous Materials Safety Administration

ENISA Threat Landscape: 2014-2017

enisa

ENISA Threat Landscape 2015
| January 2016

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	⊃	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	⊃	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
11. Insider threat	⊃	11. Data breaches	⊃	↓
12. Information leakage	↑	12. Identity theft	⊃	↑
13. Identity theft/fraud	↑	13. Information leakage	↑	↓
14. Cyber espionage	↑	14. Ransomware	↑	↑
15. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

enisa

ENISA Threat Landscape Report 2016
Final version | 1.0 | OPSEC | January 2017

Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	↑	1. Malware	↑	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Denial of service	↑	↑
5. Denial of service	↑	5. Botnets	↑	↓
6. Physical damage/theft/loss	⊃	6. Phishing	⊃	↑
7. Insider threat (malicious, accidental)	↑	7. Spam	↓	↑
8. Phishing	⊃	8. Ransomware	⊃	↑
9. Spam	↓	9. Insider threat (malicious, accidental)	⊃	↓
10. Exploit kits	↑	10. Physical manipulation/damage/ theft/loss	↑	↓
11. Data breaches	⊃	11. Exploit kits	↑	↓
12. Identity theft	⊃	12. Data breaches	↑	↓
13. Information leakage	↑	13. Identity theft	↓	↓
14. Ransomware	↑	14. Information leakage	↑	↓
15. Cyber espionage	↑	15. Cyber espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

ENISA Threat Landscape: 2017-2019

enisa

ENISA Threat Landscape Report 2017
ETL 2017 | 1.0 | HSA | January 2018

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	→	8. Botnets	↑	↓
9. Insider threat	→	9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

enisa

ENISA Threat Landscape Report 2018
ETL 2018 | 1.0 | External | January 2019

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	→	1. Malware	→	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	→	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	→	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	→	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	→	10. Physical manipulation/ damage/ theft/loss	→	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

ENISA Threat Landscape: 2019-2022

https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, --- Stable, ↗ Increasing **Ranking**: ↗ Going up, --- Same, ↙ Going down

NEWS

https://www.abc.net.au/news/2019-02-19/australian-army-under-cyber-attack-major-general-marcus-thompson/10822966

Senior Defence figure raises concerns about future cyber attacks — and the scenario costing him sleep

AM / By political reporter Stephanie Borys

Posted Tue 19 Feb 2019 at 6:13am, updated Tue 19 Feb 2019 at 9:50am

Major General Marcus Thompson says the military's cyber attack threat is rising. *(Supplied: Department Of Defence)*

One of Australia's senior military figures says the threat of cyber attacks against the nation's infrastructure and military networks is on the rise.

Major General Marcus Thompson leads the Information Warfare Division, which was set up in mid-2017 with the aim of providing both defensive and offensive cyber capabilities.

In his first media major interview, he told the ABC the job of protecting Australia from serious cyber threats was only becoming more challenging.

"What I'm seeing is a significant up-tick in the threats both from a criminal perspective as well as from state-sponsored [groups]," he said.

Key points:

- Major General Marcus Thompson has warned the threat of cyber attacks on the military is on the rise
- The senior Defence official has concerns about Australia's ability to handle a major attack
- Foreign hackers have gained access to the major political parties in a cyber attack

The primary responsibility of the Information Warfare Division is to defend the military's own systems, but Major General Thompson said he held concerns about the threat to civilian infrastructure.

That includes Australia's ability to respond if a major cyber attack were to be launched on critical systems such as banks, telecommunication or utility companies.

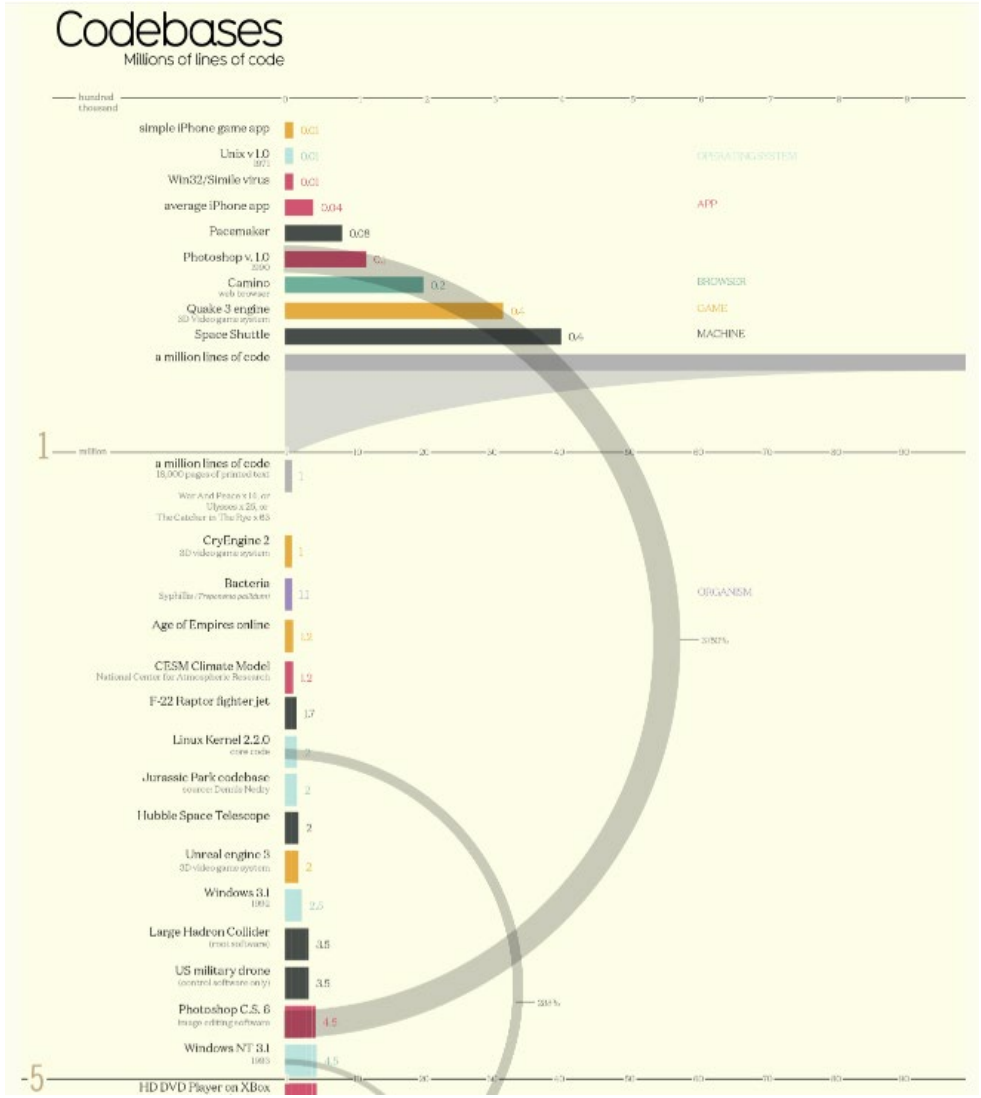
Software Vulnerabilities

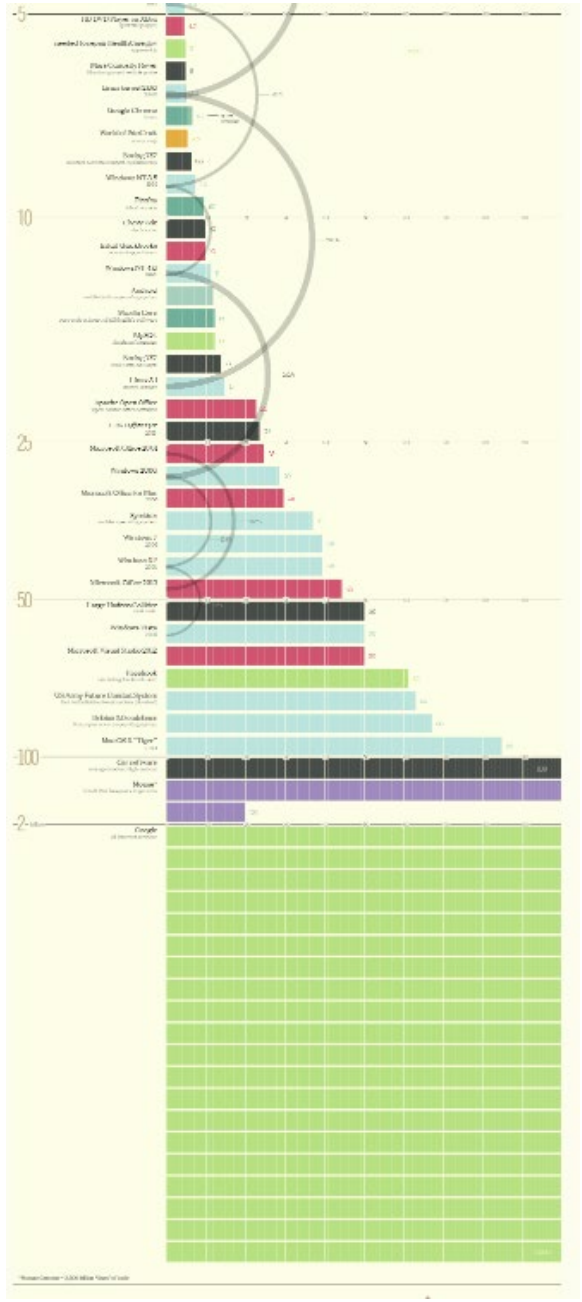
Vulnerabilities By Type

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	894	177	112	172			2	7		25	16	103			2
2000	1020	257	208	206	1	2	4	20		48	19	139			
2001	1677	403	403	297		7	34	124		83	36	220		2	2
2002	2156	498	553	435	2	41	200	103		127	76	199	2	14	1
2003	1527	381	477	372	2	50	129	60	1	62	69	144		16	5
2004	2451	580	614	408	3	148	291	111	12	145	96	134	5	38	5
2005	4935	838	1627	657	21	604	786	202	15	289	261	221	11	100	14
2006	6610	893	2719	666	91	967	1302	322	8	267	272	184	18	849	30
2007	6520	1101	2601	954	95	706	883	338	14	267	326	242	69	700	45
2008	5632	894	2310	699	128	1101	807	362	7	288	268	188	83	170	76
2009	5736	1035	2185	698	188	963	852	323	9	337	302	223	115	138	738
2010	4653	1102	1714	671	342	520	605	276	8	234	284	238	86	73	1501
2011	4155	1221	1334	723	351	294	470	109	7	197	408	206	58	17	557
2012	5297	1425	1459	828	423	243	759	122	13	344	391	250	166	14	623
2013	5191	1455	1186	846	366	155	650	110	7	352	510	274	123	1	206
2014	7939	1599	1572	839	420	304	1103	204	12	457	2107	239	264	2	403
2015	6504	1793	1830	1081	749	221	784	151	12	577	752	366	248	5	129
2016	6454	2028	1496	1219	717	94	498	99	15	444	866	601	86	7	1
2017	14714	3157	3004	2465	745	508	1518	278	11	629	1638	459	327	18	6
2018	16557	1855	3041	2120	400	517	2048	544	11	708	1227	247	461	31	4
2019	17344	1345	3201	1244	488	552	2391	475	10	712	915	202	535	57	13
2020	18325	1352	3251	1528	409	464	2183	415	14	966	1200	310	402	37	62
2021	20171	1838	3851	1660	483	741	2714	532	5	879	777	261	505	46	
2022	25227	2054	4063	2234	421	1789	3407	694	8	1049	680	214	744	54	
2023	4324	329	709	370	57	376	736	116	3	177	97	141	115	14	
Total	196013	29610	45520	23392	6902	11367	25156	6097	202	9663	13593	6005	4423	2403	4423
% Of All		15.1	23.2	11.9	3.5	5.8	12.8	3.1	0.1	4.9	6.9	3.1	2.3	1.2	

https://www.cvedetails.com/vulnerabilities-by-types.php

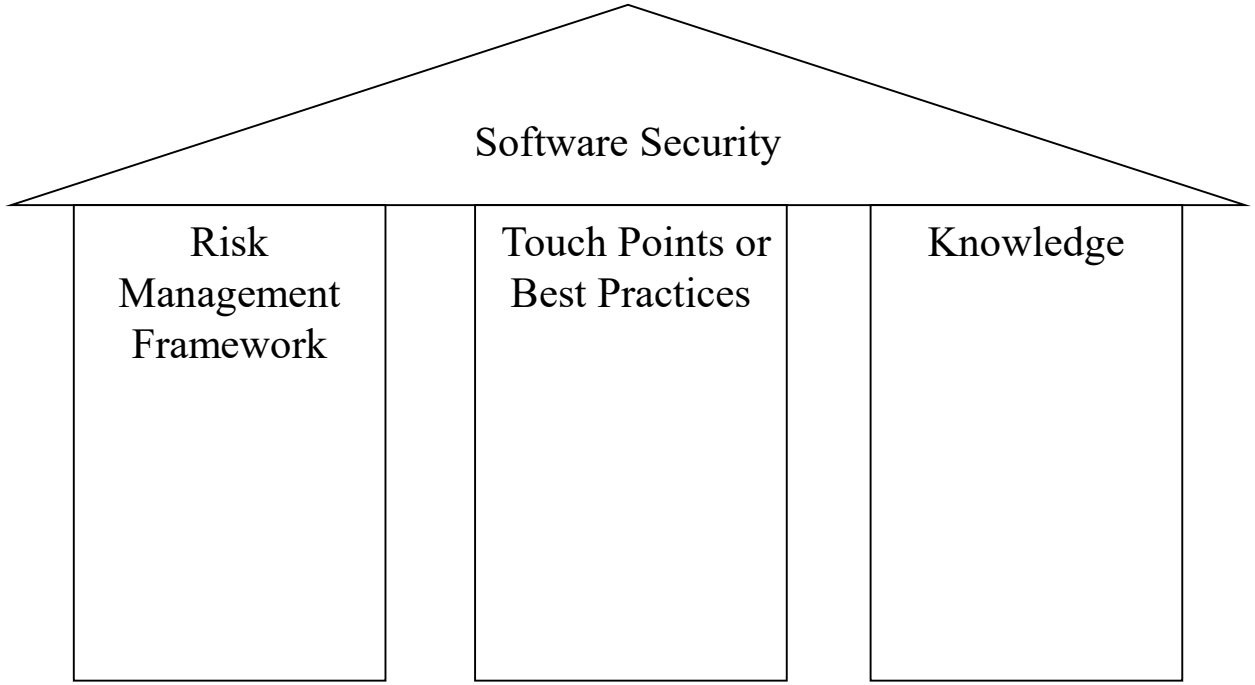
Code Size





https://informationisbeautiful.net/visualizations/million-lines-of-code/

Software Security



- Adopted by
  - US govt in National Cyber Security Task Force report
  - Cigital
  - U.S Department of Homeland Security
  - Ernst and Young

Risk Management Framework

- Overall approach to risk management is important
- At a high level it is a business-level decision
- A good judgement call based on the knowledge

Touch Points or Best Practices

- Software security is a system-wide issue
- Security is an emergent property of software system
- Not necessary that problem is due to failure of security mechanism
- Hence software security must be part of full life cycle approach
- Need to build security in

Knowledge

- Knowledge management & training play critical role in encapsulating and spreading emerging discipline
- Knowledge catalogs
- Knowledge can be applied in various stages in SDLC
- One effective way is through the use of best practices

Risk Management Framework

- Purpose is to consistently track and handle risks

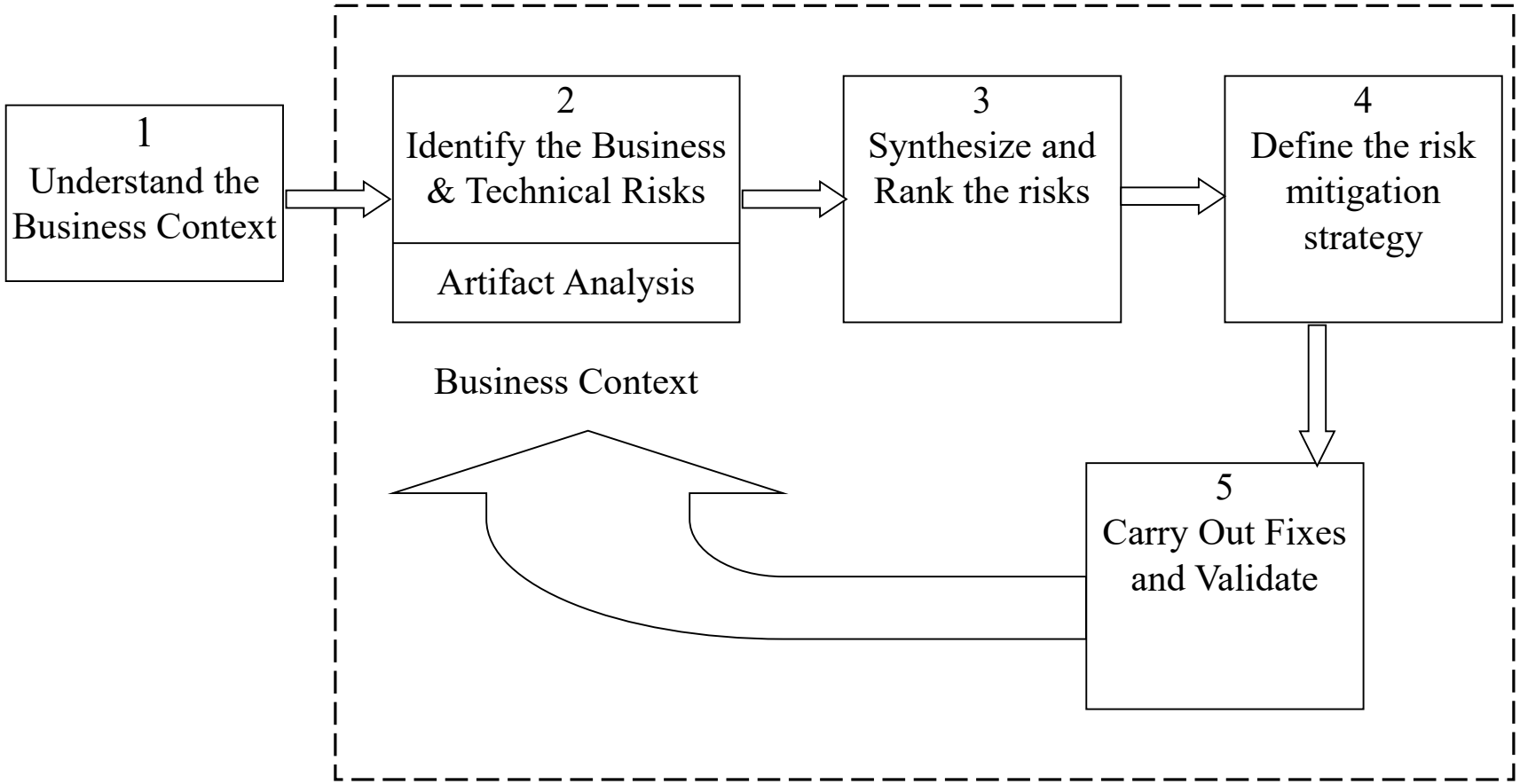
- Five stages of activity
  - Understand the business context
  - Identify business & technical risks
  - Synthesize and rank the risks
  - Define risk mitigation strategy
  - Carry out fixes and validate

- Measuring & reporting on risk

- RMF is a multilevel loop

- Can be manual or automated process

Risk Management Framework



Risk Management Framework

- Understand the business context
  - Risks are unavoidable
  - Management of risks deeply impacted by business motivation
  - Getting handle on business situation
  - Commonly business goals not explicitly stated
  - Difficulty expressing the goals clearly
  - Business goals include: meeting SLA, reducing development costs, generating high ROI
  - Purpose is to gather data to answer “who cares?” question

Risk Management Framework

- Identify the business and technical risks
  - Business risks threaten one or more business goals
  - Identification of risks helps to quantify how the events can impact business goals
  - Business impact: financial loss, damage to brand or reputation, violation of customer or regulatory constraints, exposure to liability, increase in development costs
  - Severity of business risk should be expressed in financial or project management terms
  - Example: market share, direct cost, level of productivity & cost of rework

Risk Management Framework

- Identify the business and technical risks (continued)
  - Business risk identification
    - helps to define and steer use of particular technical methods for extracting, measuring, and mitigating software risks
    - Provides necessary foundation that allows software risk to be quantified and defined in business terms
    - Makes impact statements tangible and spurs action on risk management
  - Key to risk management: tying technical risks to business context in meaningful way
  - Needs expertise to identify & understand risks

Risk Management Framework

- Synthesize and Rank the risks
  - Large number of risks apparent in any given system
  - Identification of risks is important but prioritisation of risks leads directly to creation of value
  - “who cares?” question must be answered
  - Prioritisation must take into account
    - which business goals are most important to organisation
    - which goals are immediately threatened
    - how likely are the technical risks

Risk Management Framework

- Define the Risk Mitigation Strategy
  - Problem: Analysts are good at finding technical problem but difficult to determine what to do with them
  - Risk analysis is only good as the mitigation strategy it contains
  - Create coherent strategy for mitigating threats in cost-effective manner
  - Take into account implementation time, likelihood of success, completeness, and impact over entire corpus of risks
  - Risk mitigation strategy
    - must be constrained by business context
    - Consider what organisation can afford, integrate & understand

Risk Management Framework

- Carry Out Fixes and Validate
  - Once a mitigation strategy has been defined, it must be executed
  - Identified problems (architectural flaws, coding errors, problems in testing) have to rectified
  - Risk mitigation is carried out according to strategy defined in previous step
  - Progress measured in terms of completeness against the risk mitigation strategy

Risk Management Framework

- Measuring and Reporting on Risk
  - Very important: central activity of identifying, tracking, storing, measuring and reporting risks
  - Need for continuous and consistent identification and storage of risk information as it changes over time
  - Master list of risk should be maintained during all stages of RMF execution and continuously revisited
  - Measurement regarding master list & risks mitigated over time helps to track progress

Risk Management Framework

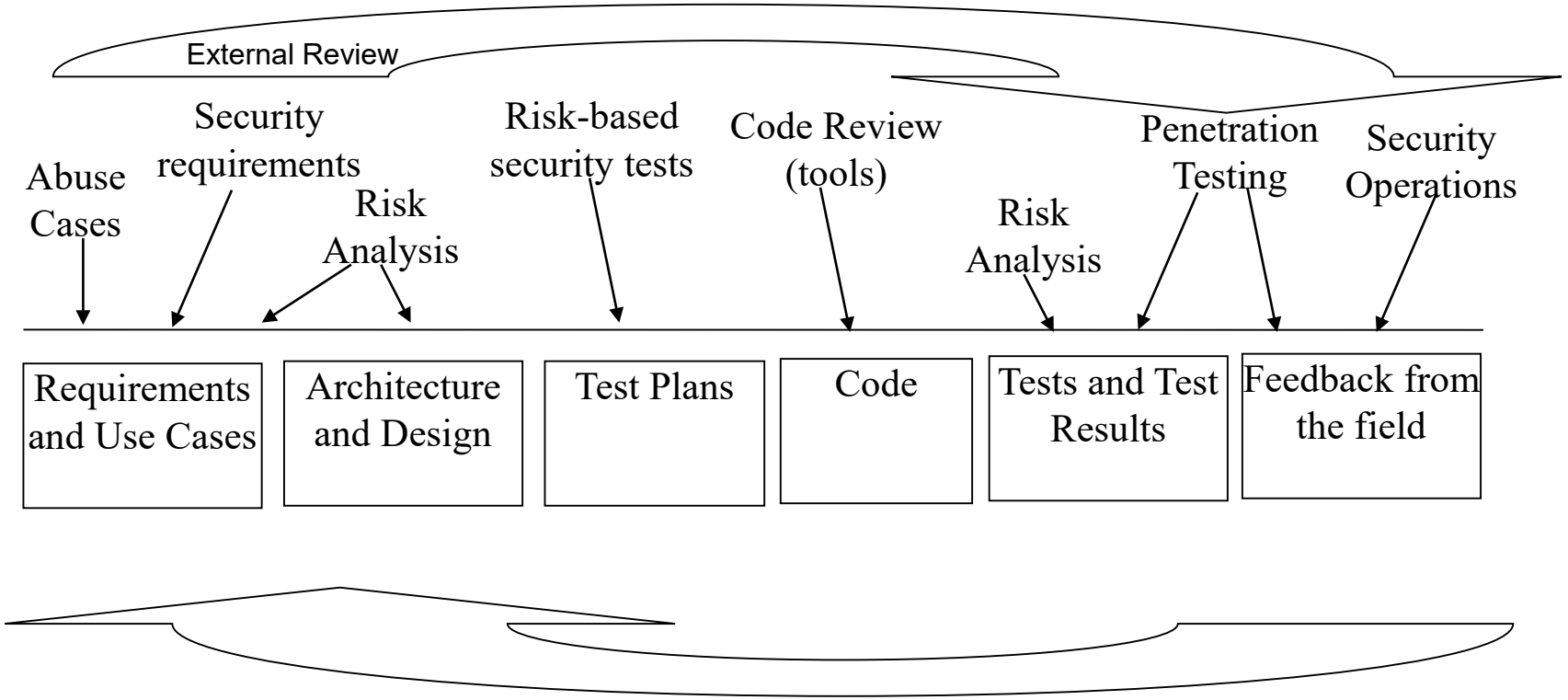
- RMF is a Multilevel loop
    - Risk management is a continuous process
    - Identifying risks only once is insufficient
    - Risks can crop at any time during the software life cycle
    - Risks can crop between stages

Best Practices

- Code Review
- Architectural Risk Analysis
- Penetration Testing
- Risk-Based Security Testing
- Abuse Cases
- Security Requirements
- Security Operations
- External Review: Not a best practise but important

Best Practices

- Code Review
- Architectural Risk Analysis
- Penetration Testing
- Risk-Based Security Testing
- Abuse Cases
- Security Requirements
- Security Operations
- External Review: Not a best practise but important



Code Review

- Artifact: Code
- Example of risks found: Buffer overflow on line 10
- All software projects produce code
- Focus is on implementation bugs that can be discovered by static analysis tools
- Very useful activity and can uncover about 50% of problems
- Code review is necessary but not sufficient
- Cannot find architectural problems
- Need for combining code review and architectural analysis

Code Review: Source Code Analysis tools

- Static tools characteristics
  - Be designed for security
  - Support multiple tiers
  - Be extensible
  - Easy to use
  - Useful for security analysts and developers
  - Support existing development process
  - Educate developers in secure coding practice
  - Should have minimal false alarms
- Depends on the knowledge built into it
- May not find architectural issues
- Examples: ITS4, fortify

Architectural Risk Analysis

- Artifact: Design and specification
- Examples of risks found: poor compartmentalisation and protection of critical data; failure to authenticate users and lack of access control decisions on proper context
- At the design & architectural level a system must be coherent and present unified security front
- Assumptions are to be clearly documented & identify possible attacks

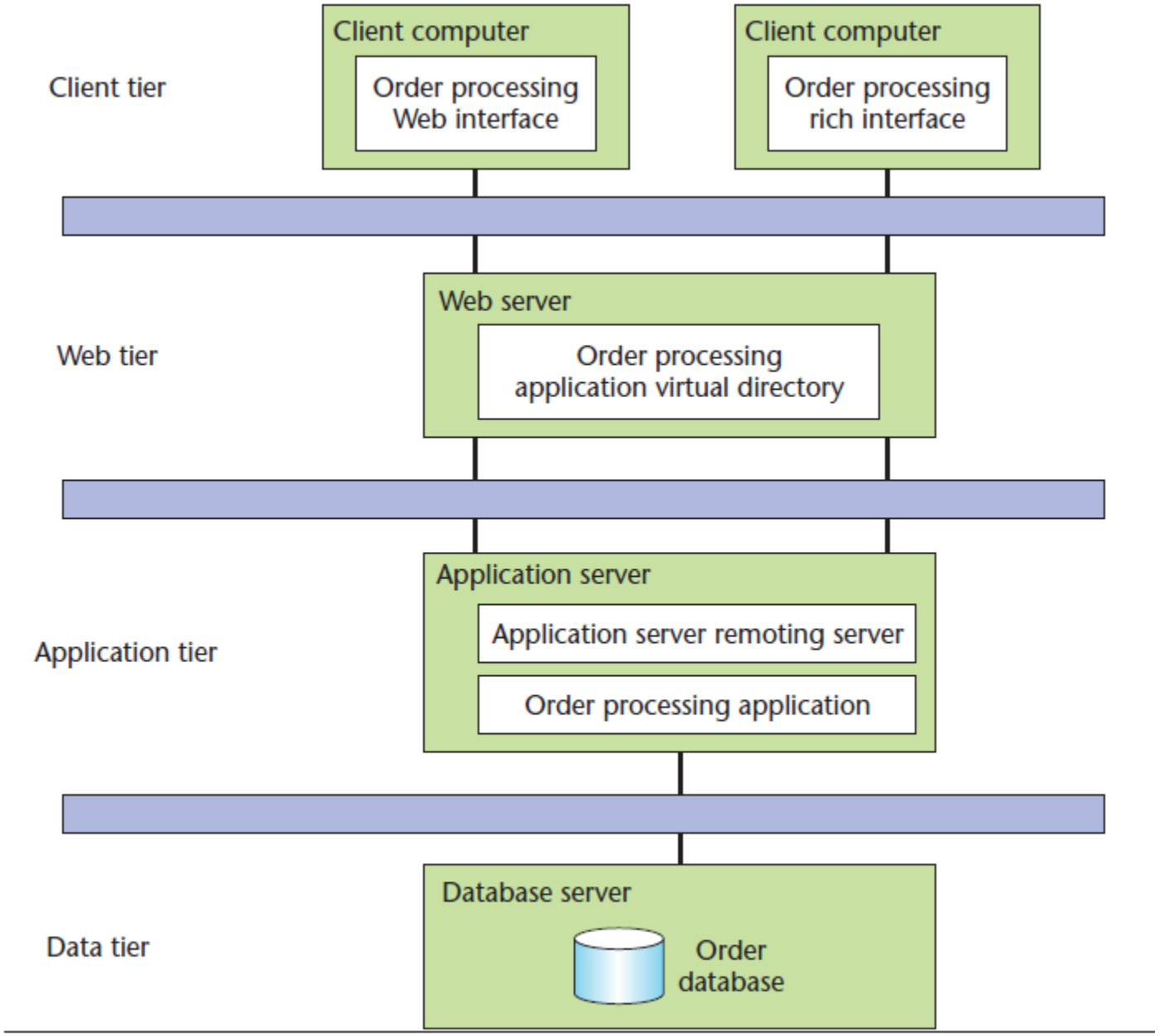
Architectural Risk Analysis

- Important for security analyst to uncover and rank architectural flaws
- Disregarding risks at this level will lead to costly problems
- Risks crop up during all stages of software life cycle
- Constant risk management thread, with recurring risk-tracking and monitoring activities is highly recommended

Architectural Risk Analysis

- Architectural risk analysis is knowledge intensive
- Business impact risks we are trying to avoid
  - Legal and/or regulatory risk
  - Financial or commercial consideration
  - Contractual considerations
- Knowledge most useful in all the steps
- Necessity of a forest-level view

Forest level view of four tier web application

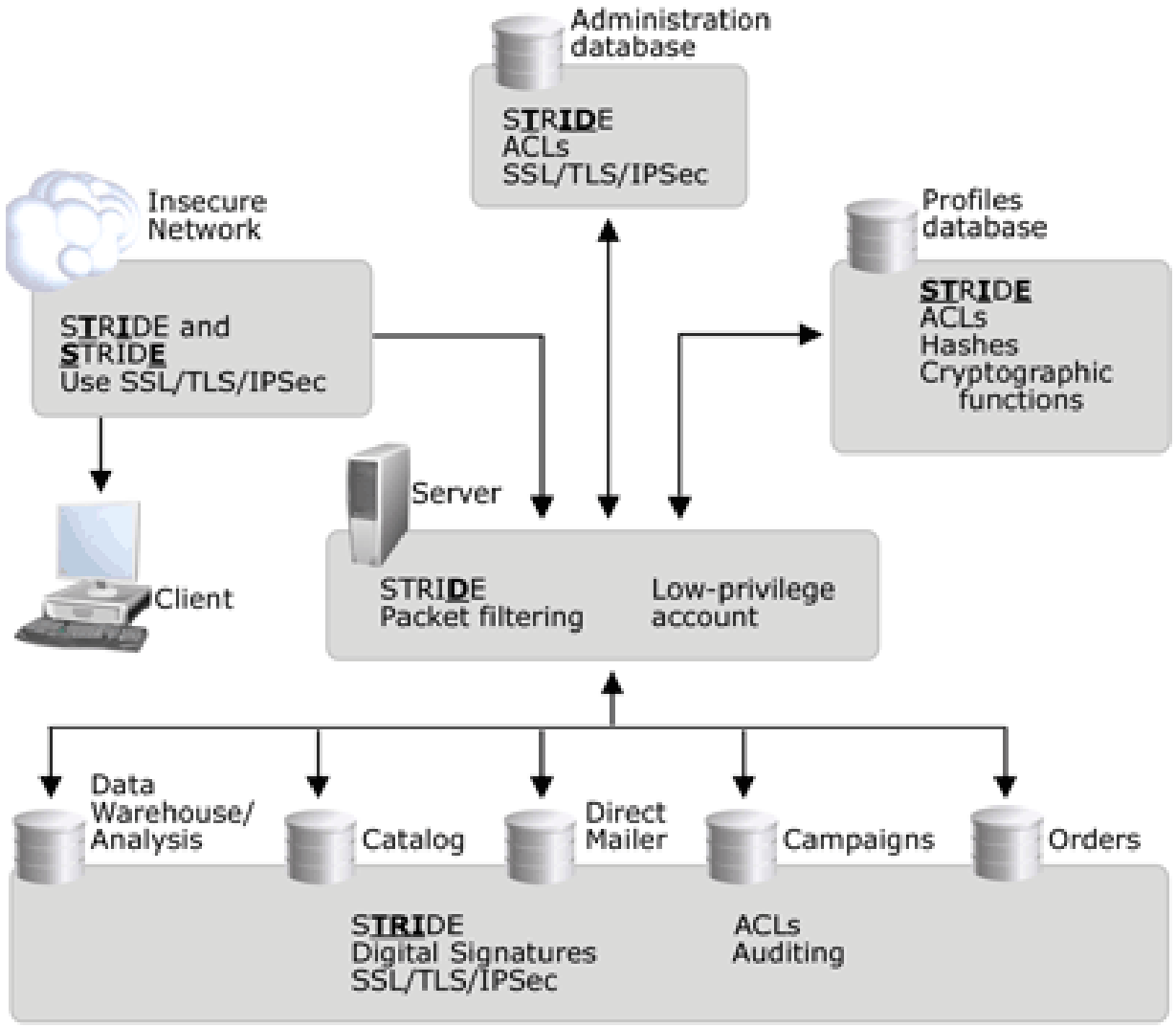


STRIDE Threat Modelling

Threat	Property Violated	Definition	Mitigation
Spoofing	Authentication	Impersonating something or someone else eg: Bob claiming to be Jane	Authentication Digital Signatures
Tampering	Integrity	Modifying something eg: modifying files or code or packets	Authorization Hashes Digital signatures Tamper-resistant protocols
Repudiation	Non-repudiation	Claiming to have not performed an action eg: if the share price goes down after purchase, then telling broker I never asked you to buy	Secure logging and auditing Digital Signatures Secure time stamps Trusted third parties
Information Disclosure	Confidentiality	Providing information to someone not authorized to see it eg: passwords transmitted in clear text	Encryption ACLS
Denial of Service	Availability	Deny or degrade service to users eg: Crashing the web site or exhausting server resources	ACLs Filtering Quotas Authorization High availability designs
Elevation of Privilege	Authorisation	Gain capabilities without proper authorization eg: A remote internet user gaining admin privileges on a webserver	ACLs Permissions Run with least privilege

Example

https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee810587(v=cs.20)



Penetration testing

- Artifact: System in its environment
- Example of risks found: poor handling of program state in web interface
- Advantages: Gives good understanding of fielded software in real environment
- One pitfall
  - Who does it
  - Be wary of reformed hackers

Risk-Based Security Testing

- Artifact: Units & System
- Example of risks found: extent of data leakage possible by leveraging data protection risk
- Risk based security testing is performed at the unit level before integration of the components
- Must encompass two strategies
  - Testing of security functionality with standard functional testing
  - Risk-based security testing based on attack patterns, risk analysis and abuse cases
- Standard QA unlikely to cover critical security issues
  - QA is about making sure good things happen
- Security testing is about making sure bad things don’t happen

Abuse Cases

- Artifact: Requirements & Use cases
- Example of risks found: Susceptibility to well-known tampering attack
- Should get into the mind of attacker
- Abuse cases describe systems behaviour under attack
- Building abuse cases requires
  - explicit coverage of what should be protected
  - from whom
  - for how long
- Underused but important

Security Requirements

- Artifact: Requirements
- Example of risks found: No explicit description of data protection needs
- Security must be explicitly worked into requirements level
- Good security requirements cover both functionality security & emergent characteristics (abuse cases & attack patterns)
- Identifying & maintaining requirements is complex
  - deserves broad treatment
  - needs expertise

Security Operations

- Artifact: Fielded system
- Example of risks found: Insufficient logging to prosecute a known attacker
- Software security can benefit from network security
- Well-integrated security operations
  - Allows network professionals to get involved in applying the best practices
  - Provide experience & security wisdom that might be missing from the development team
- Attacks happen regardless of strength of design & implementation
- Knowledge gained by understanding attacks should be recycled into software development

Knowledge for Software Security

- Key role in encapsulating & spreading the emerging discipline of software security
- Knowledge: more than the list of the things or collection of facts
- Knowledge in information in context- information put to work using processes and procedures
  - Information: list of potential security bugs in C
  - Knowledge: information built into static analysis tool
- Organise security knowledge into coherent chunks
- Experience and expertise is very valuable

Knowledge for Software Security

- Knowledge catalogs
  - Principles
  - Guidelines
  - Rules
  - Vulnerabilities
  - Exploits
  - Attack patterns
  - Historical risks
- Developers more familiar with vulnerabilities and exploits

Adopting Best Practices

- Combine your existing SDLC with best practices
- No reason to wipe the software slate clean
- Trick is to adapt your current approach according to the best practices

Business Climate

- Pressure on IT organisations to become efficient to stay competitive
- Regulatory & compliance environment is aligned with good security
- So where to start?
- Aligning software development and operational processes with strategic business objectives
- Well-architected vision and plan based on industry standards & best practices is essential
- Adoption of best practices must be tailored to given business & technical situation

Business Climate

- Build a plan that is tailored for your organisation
- Roll out individual best practice initiatives carefully
- Train your people
- Establish a metrics program
- Establish and sustain a continuous improvement capability

Building Blocks of Change

- Keeping things simple is good
- Don’t loose track of big picture
- Major change program: divide into logical segments with specific deliverables
- Allow reasonable time

Building Blocks of Change

- A stepwise approach minimises the risks & test the waters
  - Stop the bleeding: targeted at problem areas of software development
  - Harvest the low hanging fruit: quick wins
  - Establish a foundation: building blocks for future initiatives
  - Craft core competencies: current strengths & desired strengths
  - Develop differentiators: edge over competitors
  - Build out nice-to-haves : bring value