Cyber security = cyber risk management

Vulnerability

Assets & Actors

Wolter Pieters & Jan van den Berg (TUD)

3TU cyber security specialisation kickoff

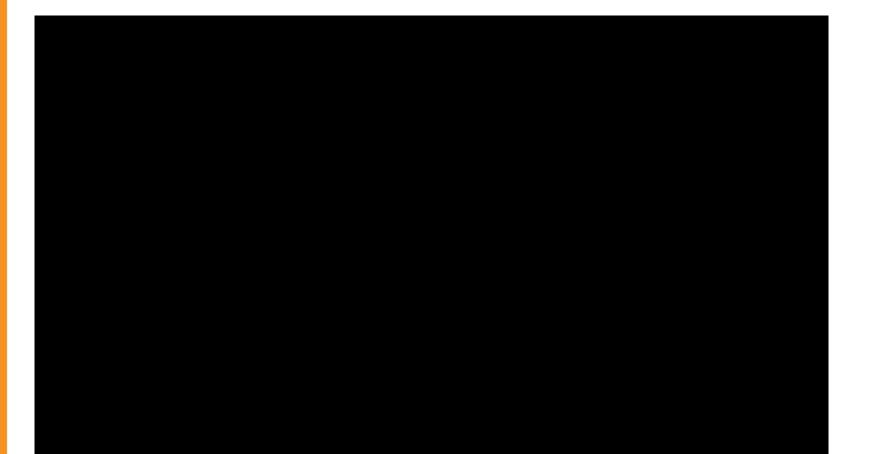
TUDelft Delft University of Technology

TU/e Technische Universiteit Eindhoven University of Technology

UNIVERSITY OF TWENTE.



Problem: voting machine chip replacement



Proposed solution: seals & non-reprogrammable chips

110 Teletekst do 12 okt

Stemcomputers veiliger door chip

Vrijwel alle stemmachines krijgen een nieuwe chip en nieuwe software die niet opnieuw te programmeren is.Een speciale commissie,met daarin ook technici,gaat het hele stemproces onderzoeken.

Minister Nicolaï heeft dat de Kamer toegezegd.Een actiegroep stelde vorige week dat de beveiliging van de meest gebruikte stemcomputer niet deugt.

Alle machines worden verzegeld met een uniek ijzeren zegel.Minister Nicolaï heeft verder de inlichtingendienst AIVD gevraagd om uit te zoeken of via radiosignalen inderdaad te achterhalen is wat iemand heeft gestemd,zoals de actiegroep claimt.

, Source: Teletekst / Wij Vertrouwen Stemcomputers Niet

Problem: Facebook invades users' privacy





Proposed solution: more privacy settings

- Hides users' personal data from each other
- But not from Facebook itself
- Encryption? But what about the business case?

Problem: vulnerability in OVchipkaart



Proposed solution: replace in 2 years time

- "Limited gain for attacker" because fraud can be detected and stopped within 2 days
- Individual fraud vs. business case for criminals

Back in 2001 (New Security Paradigms Workshop):

Information Security is Information Risk Management

Bob Blakley Tivoli Systems, Inc. blakley@us.ibm.com Ellen McDermott J.P. MorganChase Dan Geer @Stake

ABSTRACT

Information security is important in proportion to an organization's dependence on information technology. When an organization's information is exposed to risk, the use of information security technology is obviously appropriate. Current information security technology, however, deals with only a small fraction of the problem of information risk. In fact, the evidence increasingly suggests that information security technology does not reduce information risk very effectively. This paper argues that we must reconsider our approach to information security from the ground up if we are to deal effectively with the problem of information risk, and proposes a new model inspired by the history of medicine.

1. INFORMATION RISK

consequence of an event is the dollar amount of the reduction in business value which the event will cause if it occurs [Har]

1.2 Measuring Risk

A common measure of the cost of risk is "Annualized Loss Expectation," or ALE. ALE is the expected cumulative cost of risk over a period of one year as estimated in advance. For example, a chemical company estimates the probability of an explosion at one of its plants during the year 2001 as one in a million. If an explosion occurs, it will cost the company 150 million dollars in direct and indirect expenses, (for example, repair costs, legal costs, or lost business).

The ALE created by the risk of a plant explosion for the year 2001 is simply:

ALE = \$15,000,000 x (1/1,000,000) = \$150

The big question

- How do we evaluate which cyber security controls we should implement?
- Preventive, detective, responsive

Risk mitigation

- Wait until something happens
- Checklists
- Theoretical models
- Evidence-based models

Return on security investment: effectiveness & cost





Traditional risk vs. adversarial risk



Attackers

- Cryptographic assumptions: attacker cannot perform prime factorisation efficiently
- Dolev-Yao: attacker controls the network, but cannot break crypto
- Game theory: attacker maximises his utility
- Goals, skills, resources, ...

Scenarios / vulnerabilities

- Exploiting digital weaknesses
- Social engineering (e.g. phishing)
- Physical access

🖂 🛃 🗐 🍼 🥧 🔷 💗 🗢 👘 Belangrijke details (mailbox vol is) - Message (HTML)										
File Mess	sage Develope	er								۵ (?
ि Ignore X & Junk ≠ Delet	e Reply Reply	Forward 🌉 Meeting	iangleright Freedrich III Pream E-mail Pream Reply & Delete	➡ To Manager ✓ Done ♥ Create New	•	Move	Paules ▼ M OneNote Actions ▼	🗟 Mark Unread 🔡 Categorize ▾	Translate ↓ Select →	Zoom
Delete Respond		Quick Steps		E.		Move	Tags 🕞	Editing	Zoom	
You forwarde From:	d this message on	26-8-2015 11:07.							Sent: wo 26-8-2	2015 10:57
To: Cc: Subject: Be	langrijke details (m	nailbox vol is)								
										_

Uw mailbox heeft zijn opslagruimte opgegeven door de beheerder overschreden, en u zult niet in staat zijn om nieuwe e-mail te ontvangen, totdat u bevestigen. Valideren -> kopiëren, of klik hier <u>http://webmail111.moonfruit.com/</u>

*

Possible controls

- More crypto
- Hardening / patching
- Locks / cards / biometrics
- Training



Factors

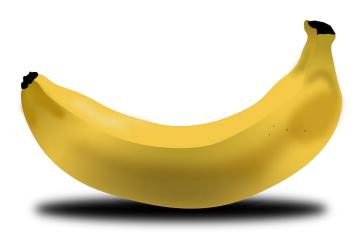
- How to combine system, attackers and possible controls in making security decisions?
- Can there be "evidence-based security" as there is evidence-based medicine?



Would you eat bananas?

"If you don't eat bananas, you might be robbed"

(Herley & Pieters 2015)



Key takeaways

- It's not only about theoretical effectiveness of controls, but about their contribution to the system as a whole
- Interesting achievements and challenges in measuring and predicting such contribution
- See the upcoming courses!
- CRM course: <u>http://homepage.tudelft.nl/e7x9k/CRM/</u>