The Vienna Programme

A Global Strategy for Cyber Security

Stefan Schumacher

www.sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

DeepSec 2012 Vienna

About me

- President of the Magdeburg Institute for Security Research
- Editor of the Magdeburger Journal of Security Research
- Freelance Security Consultant
- ex-NetBSD developer
- B.A. Educational Science and Psychology
- Focus on Social Engineering, Security Awareness, Organizational Security
- Veteran of several cyber wars ;-)

#include<disclaimer.h>

- This Talk is a Basis for Discussion.

The Problem

- IT emerges into more fields every day
- IT insecurity emerges into more fields every day
- Security is not a hot toppic :-(
- Let's change it.
- Let's create a strategy to do so.

Table of Contents

On Cyber Strategy

- Tactics is the theory of the use of military forces in combat.
- Strategy is the theory of the use of combats for the object of the war.
- War is a mere continuation of policy by other means.
- *It may sound strange, but for all who know War in this respect it is a fact beyond doubt, that much more strength of will is required to make an important decision in strategy than in tactics.*

On Cyber Strategy

- Tactics is the theory of the use of military forces in combat.
- Strategy is the theory of the use of combats for the object of the war.
- War is a mere continuation of policy by other means.
- *It may sound strange, but for all who know War in this respect it is a fact beyond doubt, that much more strength of will is required to make an important decision in strategy than in tactics.*

Example

- CORE-2007-0219: OpenBSD's IPv6 mbufs remote kernel buffer overflow
- develop a patch
- roll it out (`cvs update -dP`)
- patch the source and compile it
- install new version
- that's tactic, it does solve this specific IPv6 mbufs remote kernel buffer overflow
- but it does not prevent future buffer overflow

Example

- CORE-2007-0219: OpenBSD's IPv6 mbufs remote kernel buffer overflow
- develop a patch
- roll it out (`cvs update -dP`)
- patch the source and compile it
- install new version
- that's tactic, it does solve this specific IPv6 mbufs remote kernel buffer overflow
- but it does not prevent future buffer overflow

On Cyber-War

how to reach goals: Cathedral vs. Bazaar

I love it when a plan comes together Hannibal

No plan survives the first contact with the enemy - MacGyver

The Elders of the Internet

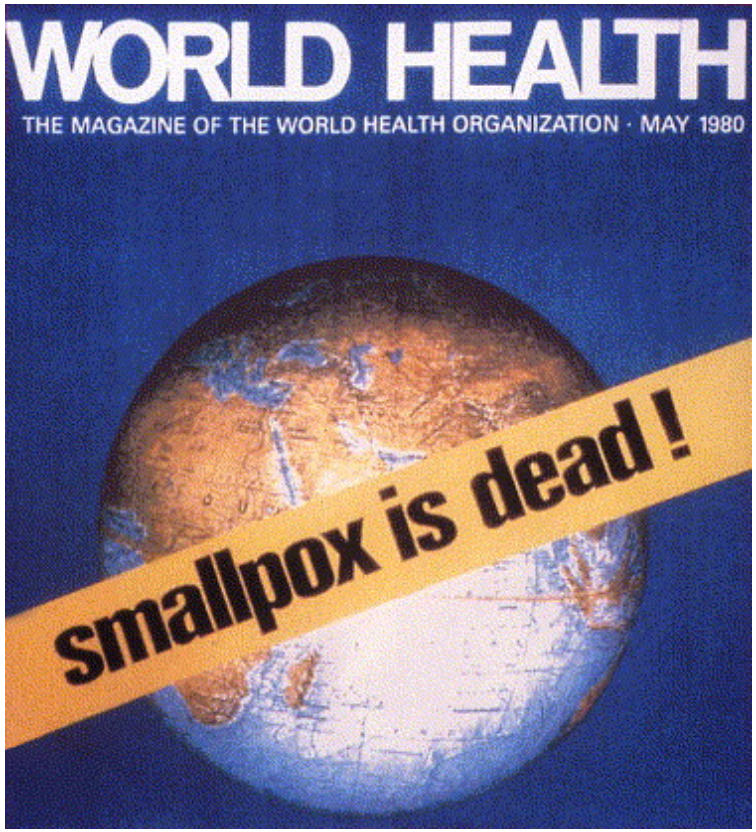
- We need some global kind of organization
- in all dimensions (technical, psychological, social, juridical, international law)
- some institutions already exist (BSI, ENISA)
- coordination is required (think of the United Nations `not` ITU)
- why not organizing like an open source project? (Bazaar)
- Wikipedia: offer a Wiki/Mailing List/Forum etc. for discussion
- NetBSD: steering committee, developer groups, mailing listes, sponsors for new developers, security officers

The Elders of the Internet

- information security is not only a technical problem
- involve *all* actors: international organizations, governments, political parties, citizens/users, developers, researchers, companies
- get some Second Order Cybernetics (discourse analysis, institutional analysis, governance etc., see Luhmann, von Foerster)
- fight the Semmelweis-Reflex (reflex-like tendency to reject new knowledge because it contradicts established norms)

Table of Contents

Malware? What's that?



The World Health Organization eradicated Smallpox in the 1970s and Rinderpest in 2011

They had a strategy

Malware? What's that? Do you Remember?

- Let's eradicate Malware.
- Ain't that megalomanic? Sure, but we need big goals ...
- We know the complete »DNA« of every OS/Application, we can even change it
- We can reverse engineer the DNA of malware or create our own examples in the lab
- We can even mathematically verify the absence of vulnerabilities
- We don't have to walk through the outback to get to our patients
- Yet we still have Buffer Overflows since 1988 ...

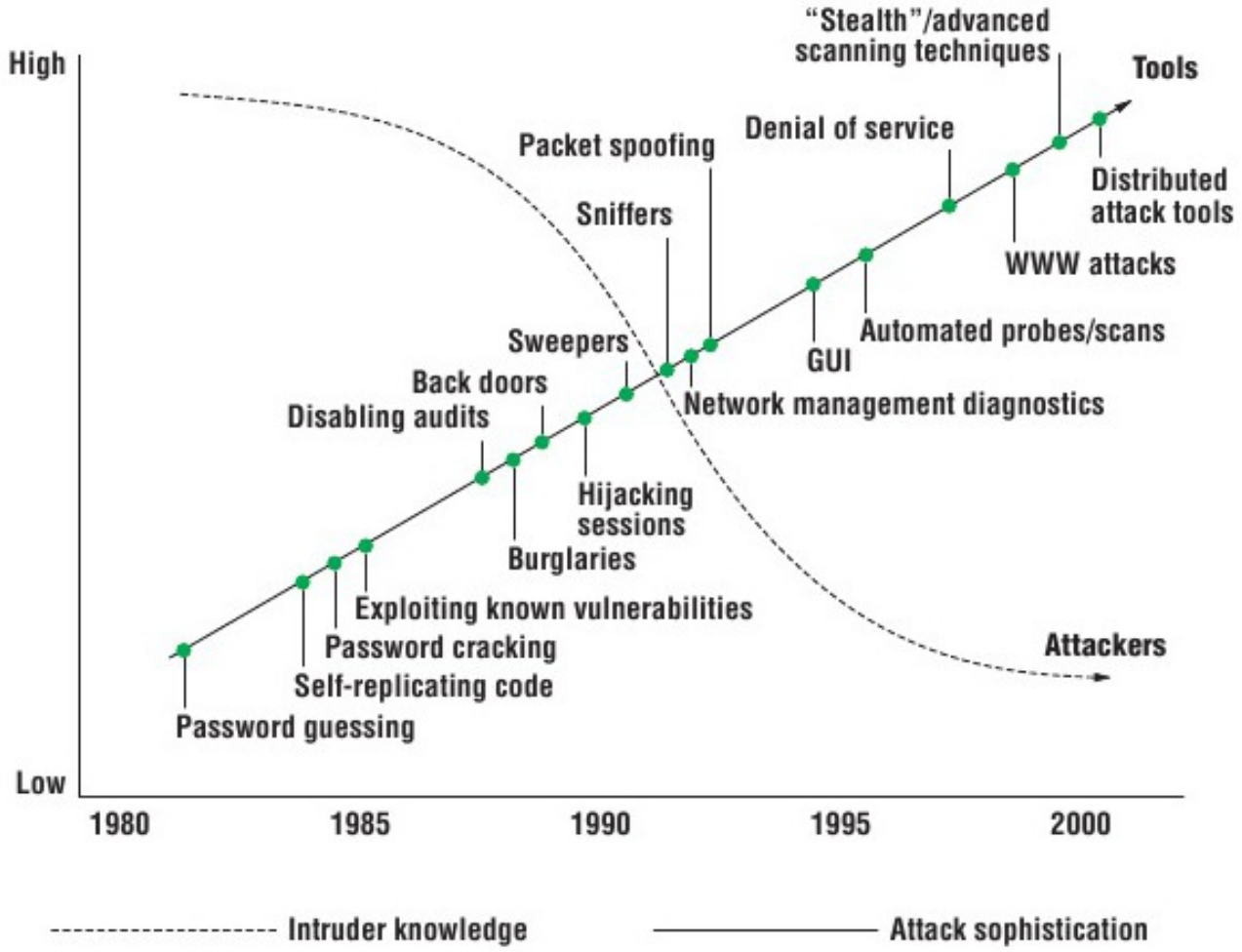
Malware? What's that? Do you Remember?

- Let's eradicate Malware.
- Ain't that megalomanic? Sure, but we need big goals ...
- We know the complete »DNA« of every OS/Application, we can even change it
- We can reverse engineer the DNA of malware or create our own examples in the lab
- We can even mathematically verify the absence of vulnerabilities
- We don't have to walk through the outback to get to our patients
- Yet we still have Buffer Overflows since 1988 ...

Malware? What's that?

- Identify all the simple Vulnerabilities and wipe them out
- have a look at the governance model of NetBSD and OpenBSD
- close at least the Skript Kiddie Vulnerabilities

Malware? What's that?



Commercial Software

the political/legal dimension

- prioritise security
- don't sell it as an add on: Security First
- talk to us, offer a path for responsible disclosure
- and act!
- customers have a lot of power (€€€)
- manufacterers are liable for their products
- car manufacturers have to recall malfunctioning cars
- aviation authorities monitor airlines and shut them down in case of emergency
- Has there ever been a recall for Operating Systems? Why not?
- Why do customers accept broken and FUBARed software?

Table of Contents

Psychology of Security

- Why Psychology?
- Humans act and make decisions, computers do only as told
- Programmers create Buffer Overflows and forget safety regulations (Ariane 5) ...
- Users choose weak passwords ...
- Admins forget to patch ...
- We have to influence how humans make decisions regarding IT security
- therefor we will use the ancient black art of psychology ...

Making Security Sexy

- How do I make Security »sexy«? $\rightsquigarrow$ Motivational Psychology
- The Holy Grail$^{[TM]}$ of Psychology
- a lot of research done, especially for Industrial Psychology, Leadership, Management
- motivation is the key of every action $\rightsquigarrow$ no motivation == no action
- motivation can be conscious or unconscious
- several theories of motivation

Theories of Motivation

- Maslow: Pyramid of Needs
- Herzberg: Two Factor Theory of Content
- internal vs. external Motivation
- external Motivation: Reward or Punishment
- internal motivation is the ideal way
- people have to want security on their own
- they have to focus on security
- Motivation is volatile

Security Awareness

- people only learn when they focus on something
- they focus on something that is important to them
- security has to be relevant to them
- this is a complex task: The User - An Unknown Being.
- Does he identify with his employer? (Maslow)
- What are his needs?
- Does he understand security? (Know How/Technical Skills)
- Can he integrate »security« into his mind set?
- What does his mind set look like? (Weltanschauung)

Security Awareness

- people only learn when they focus on something
- they focus on something that is important to them
- security has to be relevant to them
- this is a complex task: The User - An Unknown Being.
- Does he identify with his employer? (Maslow)
- What are his needs?
- Does he understand security? (Know How/Technical Skills)
- Can he integrate »security« into his mind set?
- What does his mind set look like? (Weltanschauung)

Weltanschauung

- externalise the mind set of an user to examine
- »get a Core Dump from his Brain for Reverse Engineering«
- qualitative research has to be done
- Psychology, Sociology, Educational Science,
- biographization, autobiographic-narrative interview, hermeneutic spiral,
- cultural influence (gun control, death by fan in Korea)
- organizational influence (police vs. advertising agency)

Personality Traits

- every individual has personality traits which are stable
- several models exist
- Motives are stable and a well researched theory in psychology
- eg.: achievement motive, power motive, affiliation motive
- Big 5 Neo FFI: Neuroticism, Extraversion, Openness, Conscientiousness, Affability
- How do personality traits correlate with security aware behaviour?
- How do traits of an organisation affect security aware behaviour?
- How do person and organisation fit together? (Person Organisation Fit)

Didactics of Security

- Didactics: science of teaching theories and methods
- professionalization science of teachers
- general didactics and subject didactics (english, math, chemistry)
- required for teaching security aware behaviour
- *How do we teach security?*
- motivation is one (important) item
- theory of action the next

Security Aware Behaviour

- several theories of action exist: Taylor, »Fordism«, Hacker, Volpert, Wygotski, Piaget, Aebli
- describe how people act and solve complex problems
- well researched field in Industrial Psychology and TVET
- How do we teach security? Material? Methods?
- What do we teach?
- Whom do we teach? (Ellyptic Curve Cryptography for everyone?)
- development of curricula
- professionals are required to assess professional competences

Didactics of Security

- fundamental research of didactics has been done
- fundamental research of technical didactics has also been done
- apply it to IT security ASAP!
- professionalize IT security training
- depending on culture and educational system
- eg: IT security curriculum for IT professions in TVET in Germany
- mandatory security course for CS/EE/Mechatronic students

Can we fix it?

What has to be done?

- talk with each other
- start a discourse
- get coordinated
- set up a road map with strategic goals
- set up a road map with tactical goals
- work to reach those goals
- reflect what we are doing
- react

Literature

Sambleben, J. und Schumacher, S. (Herausgeber). (2012). Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? Norderstedt: BoD, ISBN 9783848232703

Literature and Contact

- DeepSec Proceedings
  (submit papers or pester the speakers to do so)
- `http://www.sicherheitsforschung-magdeburg.de/journal_archiv.html`
- `stefan.schumacher@sicherheitsforschung-magdeburg.de`