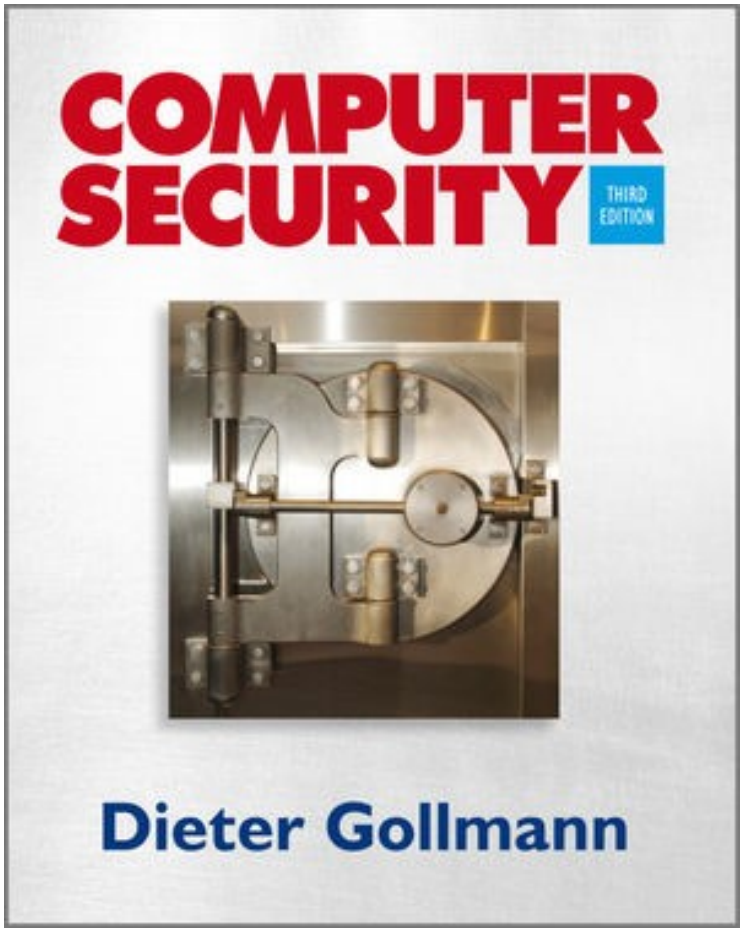
Computer Security



Info corso di Sicurezza

- Docente corso Andrea Lanzi: andrea.lanzi@unimi.it
- Pagina corso:

  http://security.di.unimi.it/sicurezza1314/
- Orario di ricevimento su appuntamento via e-mail.

Chapter 1:
History of Computer Security

Introduction

- Security is a journey, not a destination.
- Computer security has been travelling for forty years.
- The challenges faced have kept changing.
- So have the answers to familiar challenges.
- Security mechanisms must be seen in the context of the IT landscape they were developed for.

Epochs

- *1930s: people as “computers”*
- *1940s: first electronic computers*
- *1950s: start of an industry*
- *1960s: software comes into its own*
- 1970s: age of the mainframe
- 1980s: age of the PC
- 1990s: age of the Internet
- 2000s: age of the Web

Starting Point: Anderson Report, 1972

In recent years the Air Force has become increasingly aware of the problem of computer security. This problem has intruded on virtually any aspect of USAF operations and administration. The problem arises from a combination of factors that includes: greater reliance on the computer as a data processing and decision making tool in sensitive functional areas; the need to realize economies by consolidating ADP resources thereby integrating or co-locating previously separate data processing operations; the emergence of complex resource sharing computer systems providing users with capabilities for sharing data and processes with other users; the extension of resource sharing concepts to networks of computers; and the slowly growing recognition of security inadequacies of currently available computer systems.

Quoted from the Anderson report

1970s: Mainframes – Data Crunchers

- Technology: Winchester disk (IBM) 35-70 megabytes memory.
- Application: data crunching in large organisations and government departments.
- Protection of classified data in the defence sector dominates security research and development.
- Social security applications and the like.
- Security controls in the system core: operating systems, database management systems
- Computers and computer security managed by professionals.

1970s: Security Issues

- Military applications:
  - Anderson report
  - Multi-level security (MLS)
  - Bell LaPadula model
- Status today: High assurance systems developed (e.g. Multics) but do not address today's issues.
- Non-classified but sensitive applications
  - DES, public research on cryptography
  - Privacy legislation
  - Statistical database security
- Status today: cryptography is a mature field, statistical database security reappearing in data mining.

1980s: PCs – Office Workers

- Technology: Personal Computer, GUI, mouse, …
- Application: word processors, spreadsheets, i.e. office work.
- Liberation from control by the IT department.
- Single-user machines processing unclassified data: No need for multi-user security or for MLS.
- Risk analysis: no need for computer security.
- Security evaluation: Orange Book (TCSEC, 1983/85): Driven by the defence applications of the 1970s.

1980s: Security Issues

- Research on MLS systems still going strong; Orange Book, MLS for relational databases.
- Clark-Wilson model: first appearance of “commercial security” in mainstream security research.
- Worms and viruses: research proposals, before appearing in the wild.
  - Also the worm comes from Xerox park (1982) …
- Intel 80386 drops support for segmentation.

1980s: An Early Worm

- First internet worm 1988, the famous Morris's Worm
- Buffer overflow on Fingerd daemon, force password on remote login, bad configurations of Sendmail.
- The worm penetrated 5-10 \% of the machines on internet.
- The person responsible for the worm was brought to court and sentenced to a $ 10,050 fine and 400 hours of community service.

1990s: Internet – Surfers Paradise?

- Technology: Internet, commercially used.
- Applications: World Wide Web (static content), email, entertainment (music, movies), …
- Single-user machine that had lost its defences in the previous decade is now exposed to the “hostile” Internet.
- No control on who can send what to a machine on the Internet.

1990s: Internet – Surfers Paradise?

- Technology: Internet, commercially used, Web 1.0.
- Applications: Web surfing, email, entertainment, …
- Single-user machine that had lost its defences in the previous decade now exposed to “hostile” Internet.
- No control on who can send what to a machine on the Internet.
- Buffer overrun attacks:
  - Aleph One (1996): Smashing the Stack for Fun and Profit
- “Add-on” security controls: firewalls, SSL, browser sandbox as reference monitor, …

1990s: Security Issues

- Crypto wars: is wide-spread use of strong cryptography a good idea?
  - Internet security treated as a communications security problem.
- Buffer overrun attacks:
  - Aleph One: Smashing the Stack for Fun and Profit
  - Internet security is mainly an end systems issue!
- Java security model: the sandbox.
- Trusted Computing; DRM
- Status today: mature security protocols (IPsec, SSL/TLS), better software security.

2000s: Web – e-Commerce

- Technology: Web services, WLAN, PKI??
- Web 2.0: dynamic content
- B2C applications: Amazon, eBay, airlines, on-line shops, Google, ...
- Criminal activity replaces “hackers”.
- Legislation to encourage use of electronic signatures.
- PKIs have not taken off; e-commerce has essentially evolved without them.

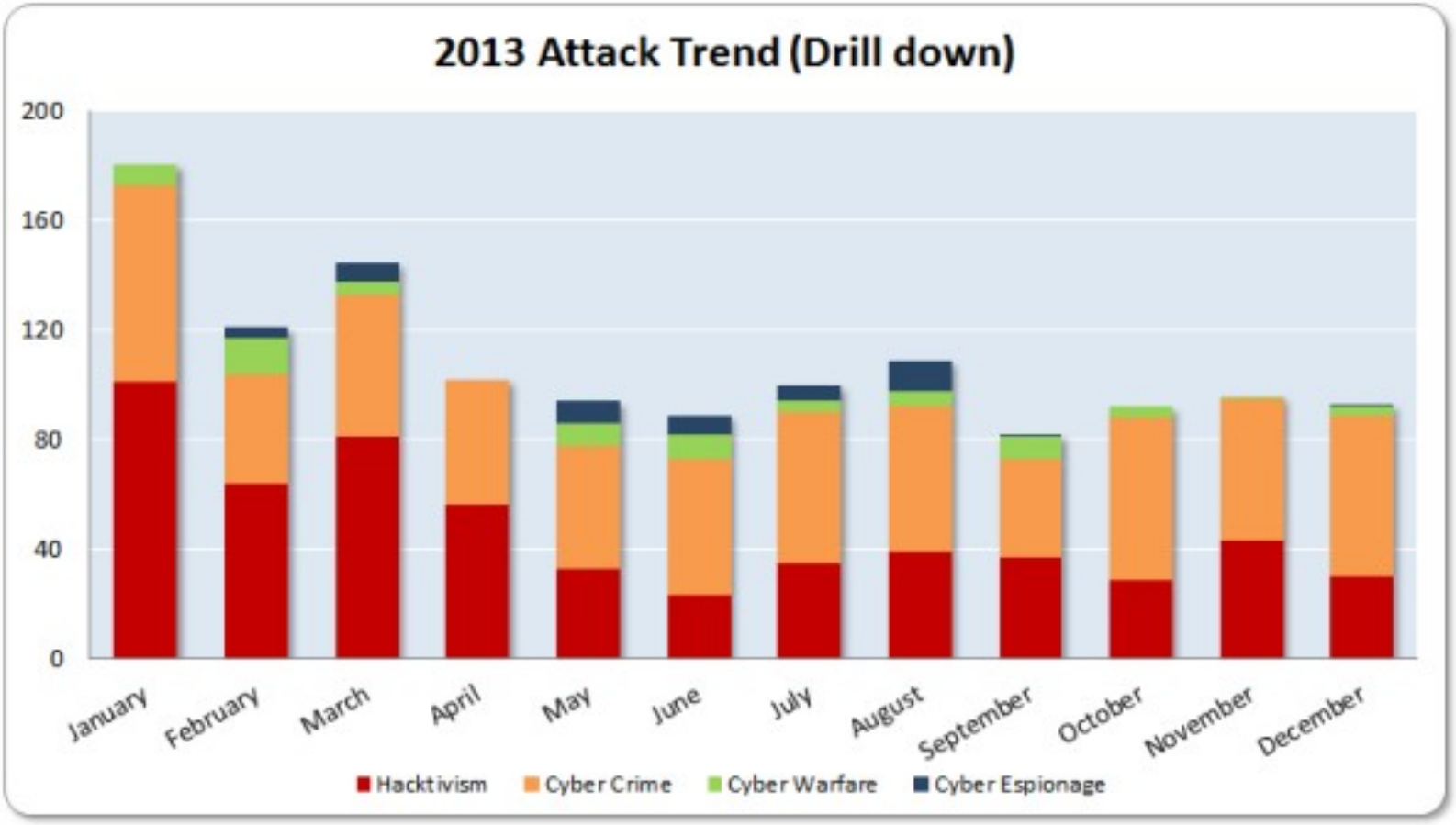
2000s: Security Issues

- SSL/TLS for secure sessions.
- Software security: the problems are shifting from the operating systems to the applications (SQL injection, cross-site scripting, DNS attack).
- Security controls moving to application layer: Web pages start to perform security checks.
- Access control for virtual organisations: e.g. federated identity management.
- Security of end systems managed by the user (take care of your system).

2000s: Security Issues

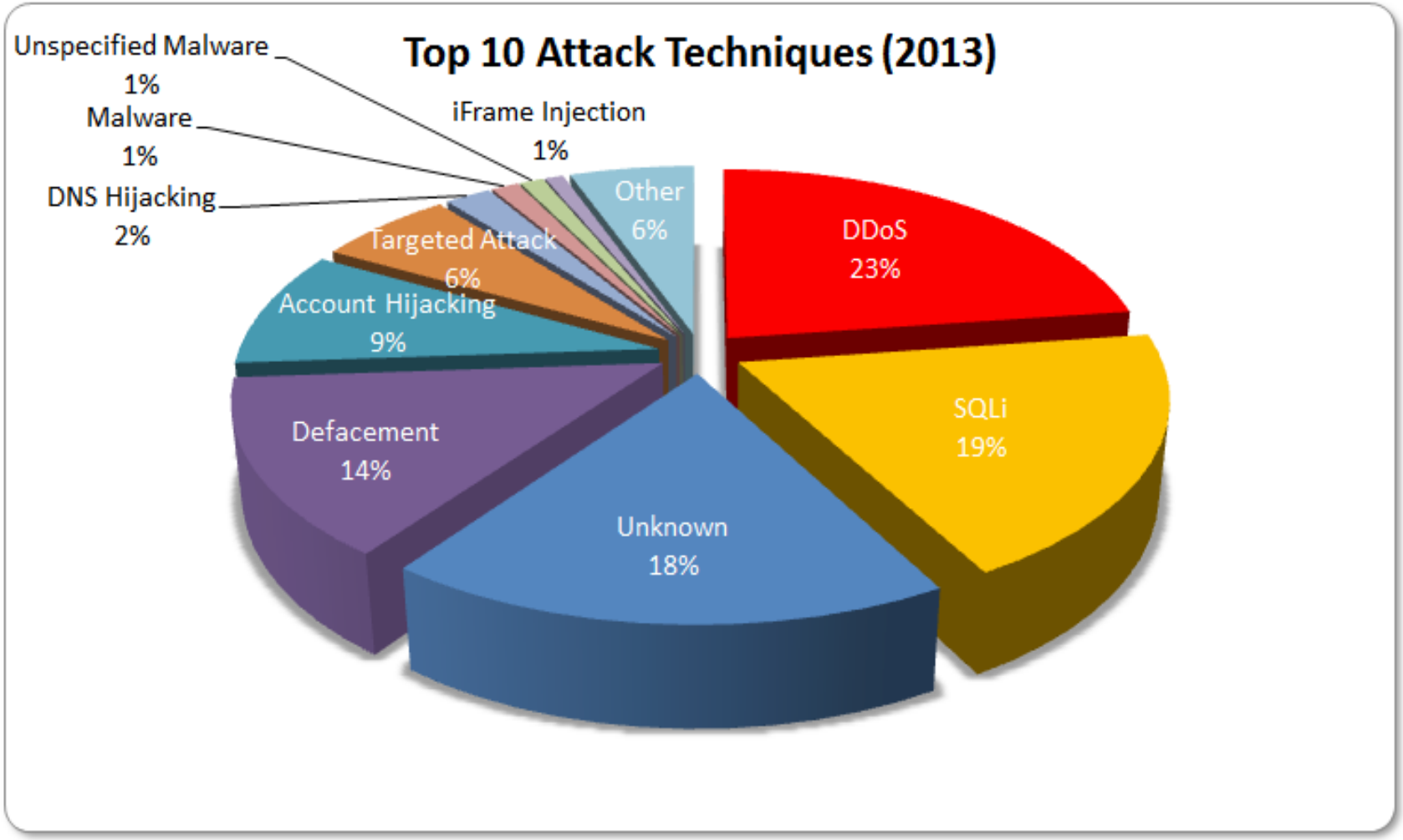
- Botnet as a new attack organization.
- CyberCrime is born which aim is to exploit technologies business to make money.
- APT attack: “Advanced persistent threat (APT) usually refers to a group, such as a government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly use to espionage using a variety of intelligence gathering techniques to access sensitive information.”
- Different actors: Cybercrimimal, Hacktivists, Governments.

2000s: Security Issues



2000s: Security Issues

2000s: Security Issues



2000s: Target Attacks

Stuxnet is a computer virus that was discovered in June 2010. It was designed to attack Siemens Step7 software running on a Windows operating system. Stuxnet almost ruined one-fifth of the Iranian nuclear centrifuge by spinning out of control while simultaneously replaying the recorded system values.

Duqu, a new worm was found, thought to be related to Stuxnet. The Laboratory of Cryptography and System Security (CrySyS) of Budapest University analyzed the malware, naming the threat Duqu. The exfiltrated data may be used to enable a future Stuxnet-like attack (2011)

2000s: Eletronic weapon

- Exploit Kit and attack companies: Hacking Team, Milan, Italy and Vupen France (0-day attack)
- They provide rootkit, zero day to the government to espionage.
- FBI Behind the attack of anonimity network TOR.

Summary

- Innovations (mouse, GUI, PC, WWW, worms, viruses) find their way out of research labs into the mass market.
- Innovations are not always used as expected: email on the Internet, SMS in GSM.
- Also the users are inventive!
- When new technology are used in innovative ways, old security paradigms may no longer apply and the well engineered ‘old’ security solutions become irrelevant.
- We can start all over again …