Introduction to Computer Security

Vítor Francisco Fonte
vff@di.uminho.pt

2021/22
Informatics Engineering Master Course
University of Minho

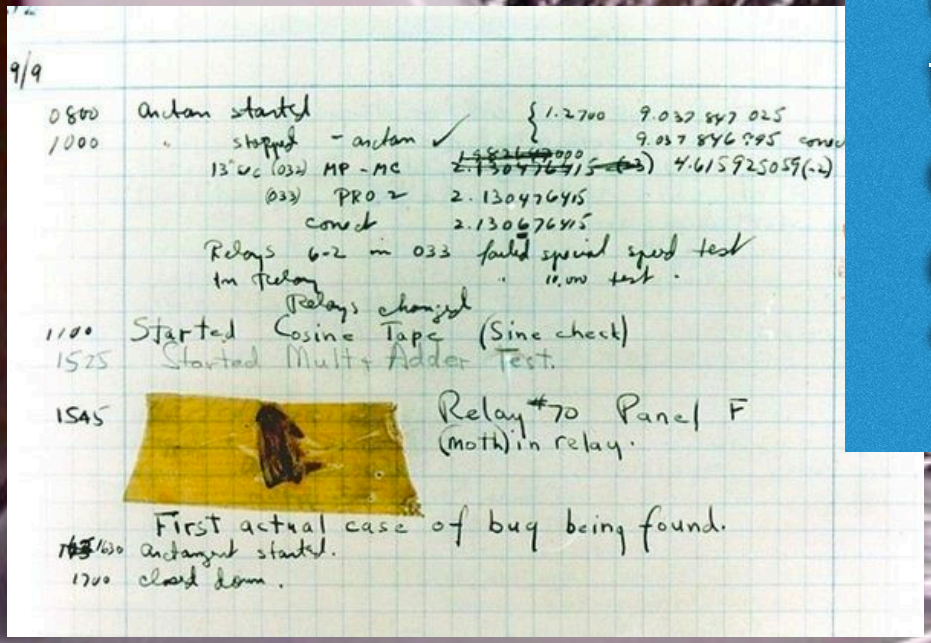
Getting started

- What is “security”?
  - different things for different people
- Original vs. current focus of computer security:
  - multiuser vs. distributed systems
  - untrusted users vs. untrusted network devices
  - keep users apart vs. protect network accessible assets
- Attacks and attackers:
  - different actors, goals and motivations
  - different methods and levels of expertise

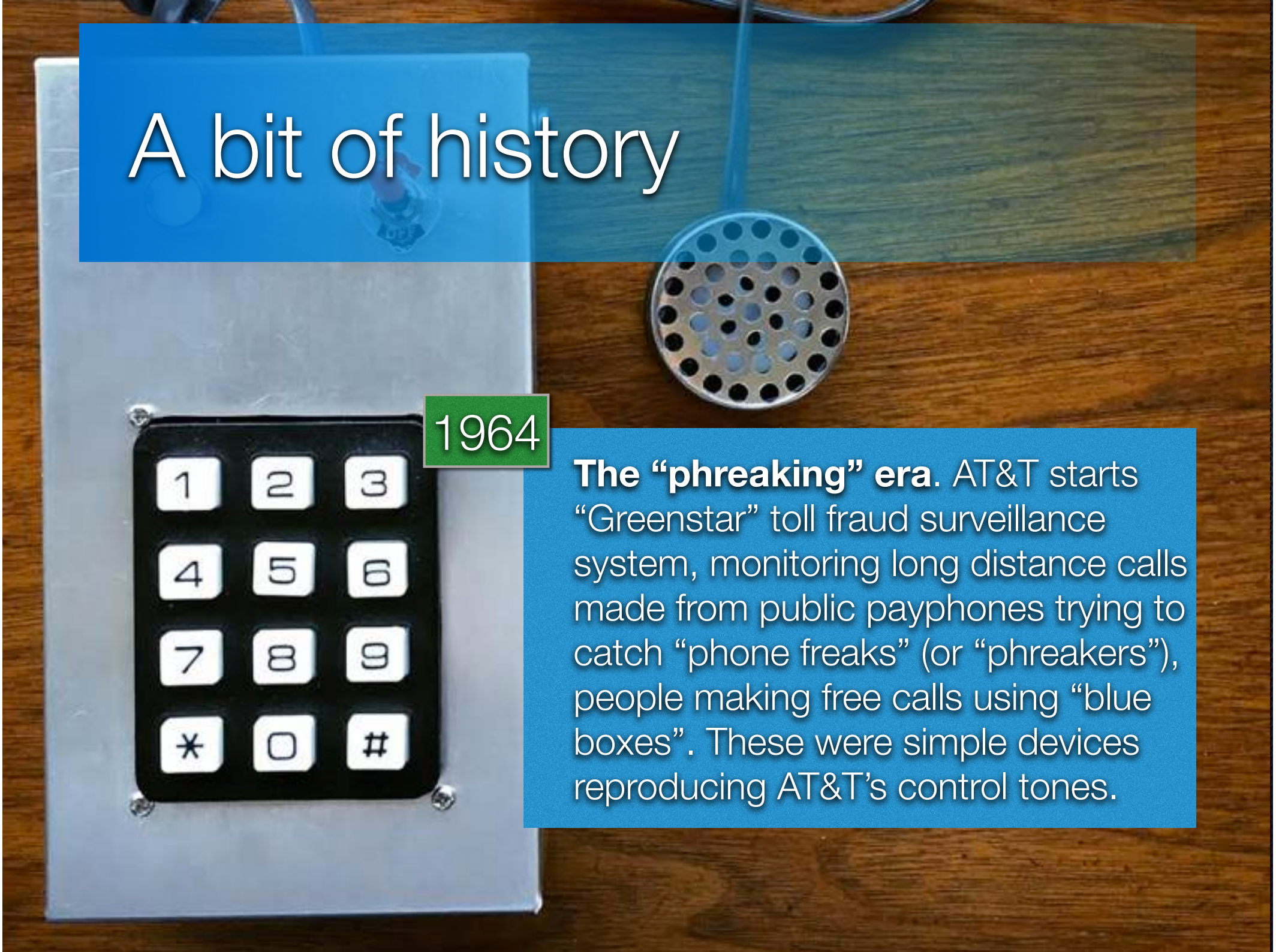
A bit of history

1945

First **“bug”.** Grace Murray Hopper records a moth being found stuck between relay contacts of a Harvard Mark II computer. Hence the terms “bug” and “debugging”.



A bit of history



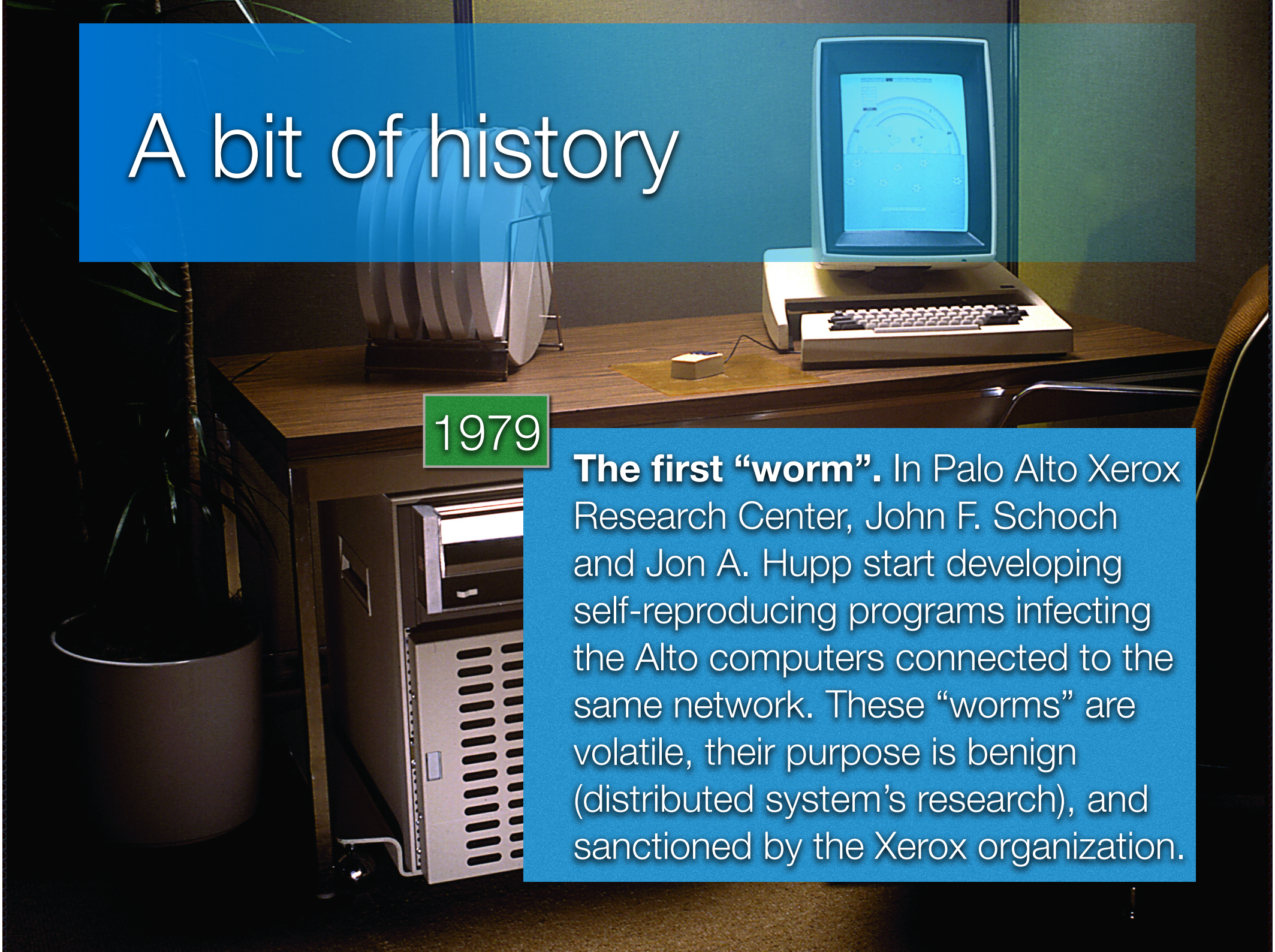
1964

The “phreaking” era. AT&T starts “Greenstar” toll fraud surveillance system, monitoring long distance calls made from public payphones trying to catch “phone freaks” (or “phreakers”), people making free calls using “blue boxes”. These were simple devices reproducing AT&T’s control tones.

A bit of history

1972

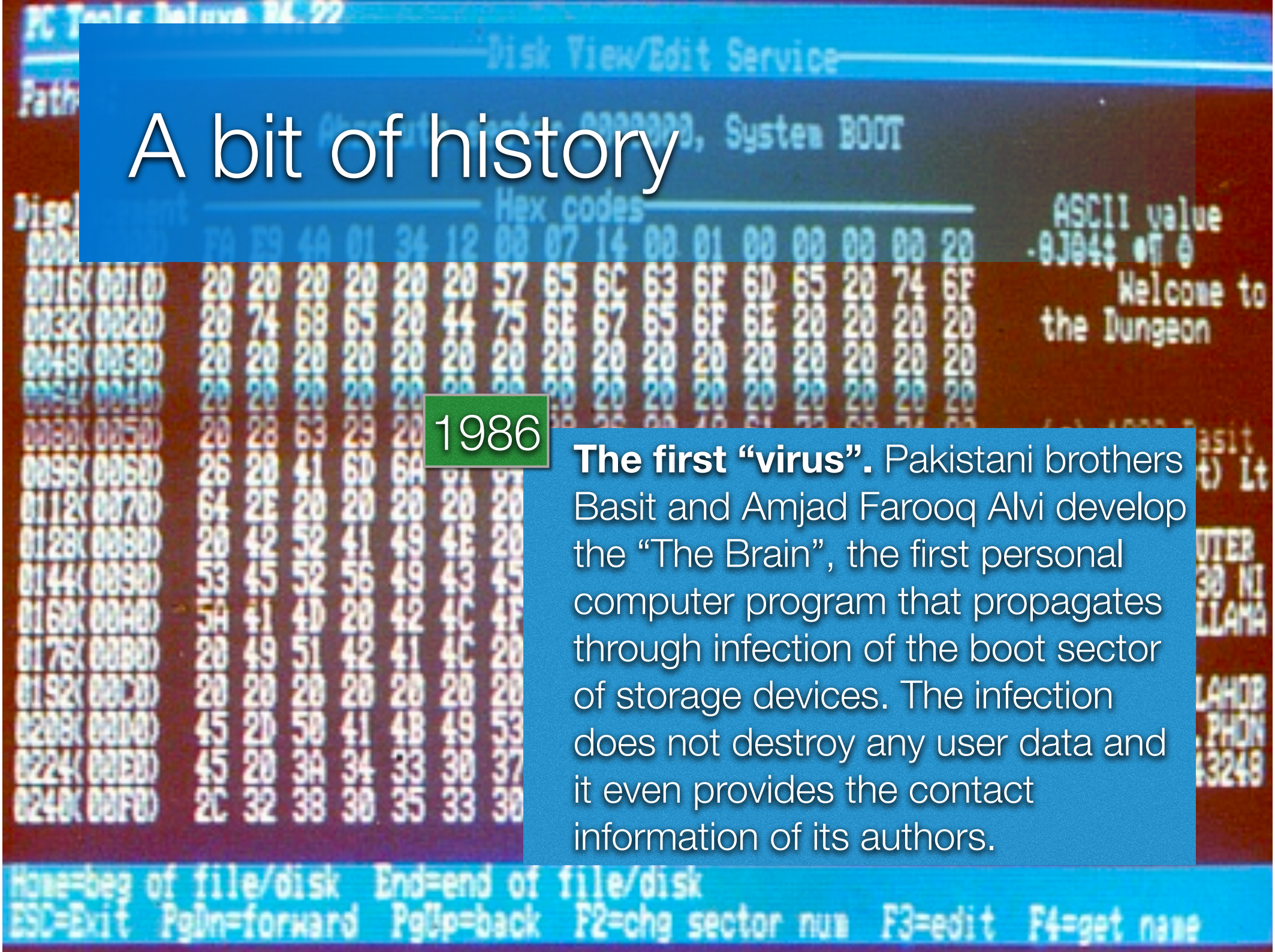
Cereal phreaking. John Drapper finds out that he could make free calls on the AT&T phone network using simply the whistle offered inside Cap'n Crunch's cereal boxes. The whistle produces a 2600Hz sound… exactly what it takes to unlock the AT&T network.



A bit of history

1979

The first “worm”. In Palo Alto Xerox Research Center, John F. Schoch and Jon A. Hupp start developing self-reproducing programs infecting the Alto computers connected to the same network. These “worms” are volatile, their purpose is benign (distributed system’s research), and sanctioned by the Xerox organization.

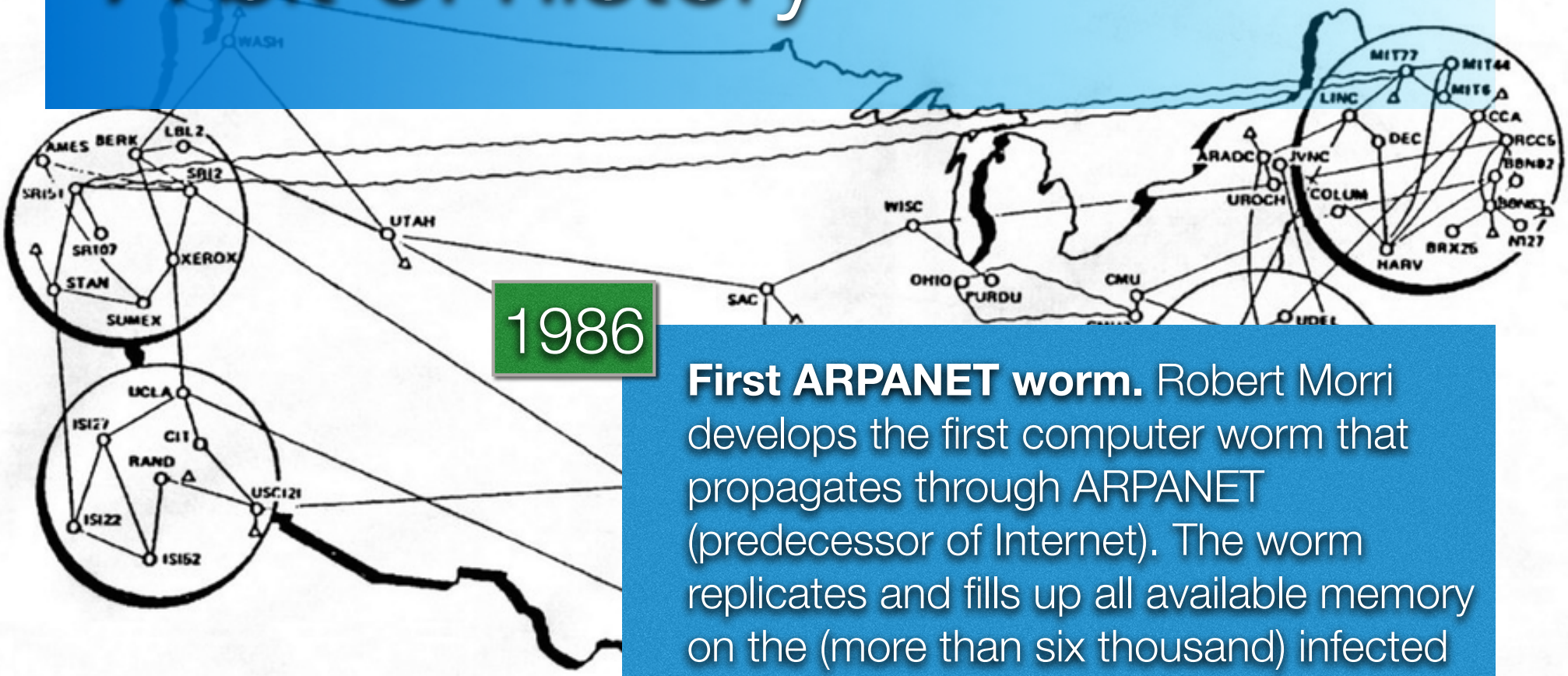


A bit of history

1986

The first “virus”. Pakistani brothers Basit and Amjad Farooq Alvi develop the “The Brain”, the first personal computer program that propagates through infection of the boot sector of storage devices. The infection does not destroy any user data and it even provides the contact information of its authors.

A bit of history



1986

First ARPANET worm. Robert Morri develops the first computer worm that propagates through ARPANET (predecessor of Internet). The worm replicates and fills up all available memory on the (more than six thousand) infected computers, rendering them inoperacional. Charged to a 3 year suspended prison sentence and a fine of 10,000 USD.

ARPANET

THE FIRST INTERNET

A bit of history

1990

First self-modifiable virus. The virus mutates with each replication rendering ineffective tradicional code signature-based detection.

1995

The first virus exploiting Microsoft Word. The “Concept” virus infects systems upon opening of a MS Word documents (via macros).

A bit of history

1998

Remote control of military and civil systems. Two US teenagers devise and execute operation “Solar Sunrise” ending up controlling more than 500 military and civil IT infrastructures.

2000

Distributed Denial of Service. Computers from the University of California are used to flood computer networks and render inoperacional sites such as Amazon, Yahoo, eBay, …

2001

“Code Red”: 2 Billion USD in damages. The worm tries to infect MS Windows NT and 2000 systems, with the end goal of a distributed attack to the White House IT infrastructure. The worm is deciphered just in time to prevent the attack.

A bit of history

2005

“PoinsonIvy”: virus and remote control in a single package. Infected systems are controlled by the malware (a remotely accessible “backdoor” is also available. It can record system activity, activate the video camera and microphone (if available.) It downloads and executes “payloads” made available from the attack remote system. It was developed in order to steal secrets from the defence and chemical industry.

2006

“Nyxem.e”: the file wiper. This worm wiped MS Office and Adobe documents (among other apps) from the infected file systems, on the third day of each month. Hundreds of users were affected.

A bit of history

2008

“Koobface”: disseminates itself via via email and social networks. It displays fake ads (eg. in Facebook) of products that once bought are never delivered to the victim.

2010

“Stuxnet”: attack to industrial control systems. Extremely complex malware that attacked specific SCADA systems. Its main victim was the Iranian nuclear enrichment infrastructure. US and Israeli intelligence agencies are suspected to have been involved in its development and deployment.

2012

“Heartbleed”: a bug in OpenSSL. This vulnerability was detected in the OpenSSL cryptographic library, and enables access to cyphered communications and stored data. Millions of systems and billions of users were affected.

A bit of history

2013

Theft of personal data of more than 70 million users. US-based Target retail business reports that a large part of its customers had their personal data records stolen from the company's computer systems.

2014

Theft of 1.2 billion authentication credetials. Russian hackers exploit (through a computer virus) vulnerabilities in the handling of SQL statements in several sites and were able to collect their users's authentication credentials. More than 500 million email accounts may have also been compromised.

Estonia, 2007

- A cyber-attack directed at a country:
  - Distributed Denial of Service: “ping flooding” using rented “botnets”
  - control of several web sites (specially in media): comment injection (spam), and content replacement(defacement)
- Affecting web sites of different institutions:
  - national parliament, ministries, media, financial institutions, …
- Considerations
  - never before seen coordination and scope
  - cyber-warfare or cyber-terrorism?

Estonia, 2007

- Considerations
  - some similarities to the Titan Rain operation (2003-06) and to the attack
  - some similarities to the attacks that took place in South Ossetia (2008)
  - network security ends up being integrated in modern militar doctrine
- Estonia deploys “digital embassies” in friendly countries
  - mitigate risks and threats to its infrastructure
  - improved redundancy: availability and integrity of data
  - business continuity: government, public admin. and service delivery

Stuxnet, 2012

- Target:
  - very specific SCADA industrial control systems
  - mainly affecting the Iranian nuclear enrichment program
- Attackers:
  - US and Israeli intel agencies suspected to be behind this attack
- Dissemination and elimination:
  - Initial infection though USB flash drives, first spotted in the wild in 2010
  - Then infecting computers in private networks not connected to the Internet
  - Set to stop and delete itself on Jan 24, 2012

Stuxnet, 2012

- Layered attack targeting:
  - Microsoft Windows operating systems executing…
  - Siemens PCS 7, WinCC and STEP7 industrial apps, running…
  - on one or more PLCs S7 from Siemens.
- Exploiting multiple vulnerabilities:
  - 4 previously unknown (0-day), extremely rare
  - 2 already unknown

Stuxnet, 2012

- Technical challenge:
  - very complex attack
  - combining different kinds of malware
  - multiple programming languages
  - user- and kernel-level (rootkit) software components
  - drivers (kernel) digital signed with valid private
  - digital keys also stolen from two Taiwanese-based companies

Snowden: NSA, 2013

- Former CIA, NSA, Dell e Booz Allen Hamilton employee
  - expert in network security and cyber-countermeasures
- Unauthorised disclosure of documents revealing secret arrangements between international intelligence agencies:
  - NSA and others US intel agencies
  - Australia (ASD), United Kingdom (GCHQ), Canada (CSEC), Denmark (PET), France (DGSE), Germany (BND), Italy (AISE), Netherlands (AIVD), Norway (NIS), Spain (CNI), Switzerland (NDB), Singapore (SID) e Israel (ISNU)

Snowden: NSA, 2013

- Global surveillance system
  - combining several agencies, tools and techniques
  - non-targeted collection of data from multiple sources (Dragnet)
  - sharing of raw data for realtime or later mining
- Main revelations:
  - secret court order grants NSA access to phone records of US citizens
  - PRISM enables direct access to the services of US tech-companies, such as Google, Facebook, Microsoft e Apple
  - GCHQ (UK) taps into fiberoptic networks all over the world
  - NSA spy on foreign countries and world leaders

Snowden: NSA, 2013

- Main revelations (continuation):
  - the Xkeyscore program can search for almost anything an user accesses and publishes on the Internet
  - the Tailored Access Operation (TAO) is a team specialised in compromising security in remote systems, infecting them with malware
  - the NSA tries to break cryptographic protocols e to undermine Internet security
  - the NSA can intercept connections to the Yahoo and Google data centres
  - the NSA intercepts the Short Message Service (SMS)
  - the NSA intercepts phone calls in the Bahamas and in Afghanistan

USA Presidential Elections, 2016

- Instrumentation of social networks
  - manipulation of social networks such as Twitter and Facebook
  - automated or manual large scale creation of user accounts
  - automated posting and sharing of fake or misleading content
  - automated sharing of content to boost its visibility (trends)
  - trending content tend to be automatically suggested to real users
  - very effective attack able to disseminate intended ideas
- The Democratic National Committee (DNC) attack
  - unauthorised access to the DNC email servers
  - leaking of sensitive emails to the media through the Wikileaks

Wikileaks: CIA #Vault7, 2017

- Tools to compromise security of smartphones (iOS and and Android), personal computers(Windows and OS X) and even cars, in order to exploit them as monitoring, listening and geo-tracking devices
- There is a secret base in Frankfurt, Germany, responsible for cyber-espionage operations in the Europe, the Middle East, and Africa
- The Weeping Angel program can exploit Samsung smart TVs and use them as listening devices even in standby
- A malware was developed in order to mask the origin/authorship of attacks, planting fake evidence of the involvement of foreign entities
- Less than 1% of documents in this treasure trove were revealed to the public

French Elections, 2017

- More than 9GB of emails and other documents were stolen from Emmanuel Macron's campaign servers
- Documents were leaked in a Russian file-sharing site
- Evidence of attempts to eliminate metadata left behind
- APT 28 is suspected to be behind these attacks
  - APT means Advanced Persistent Threat
  - APT 28 is believed to be linked to the Russian intelligence
  - APT 28 is also suspected to be have been involved in the 2016 US Presidential Elections attacks