Secure-by-Design:
Building for the User with a Security Mindset

Christine Bejerasco, CISO

WITH secure


OFFLINE

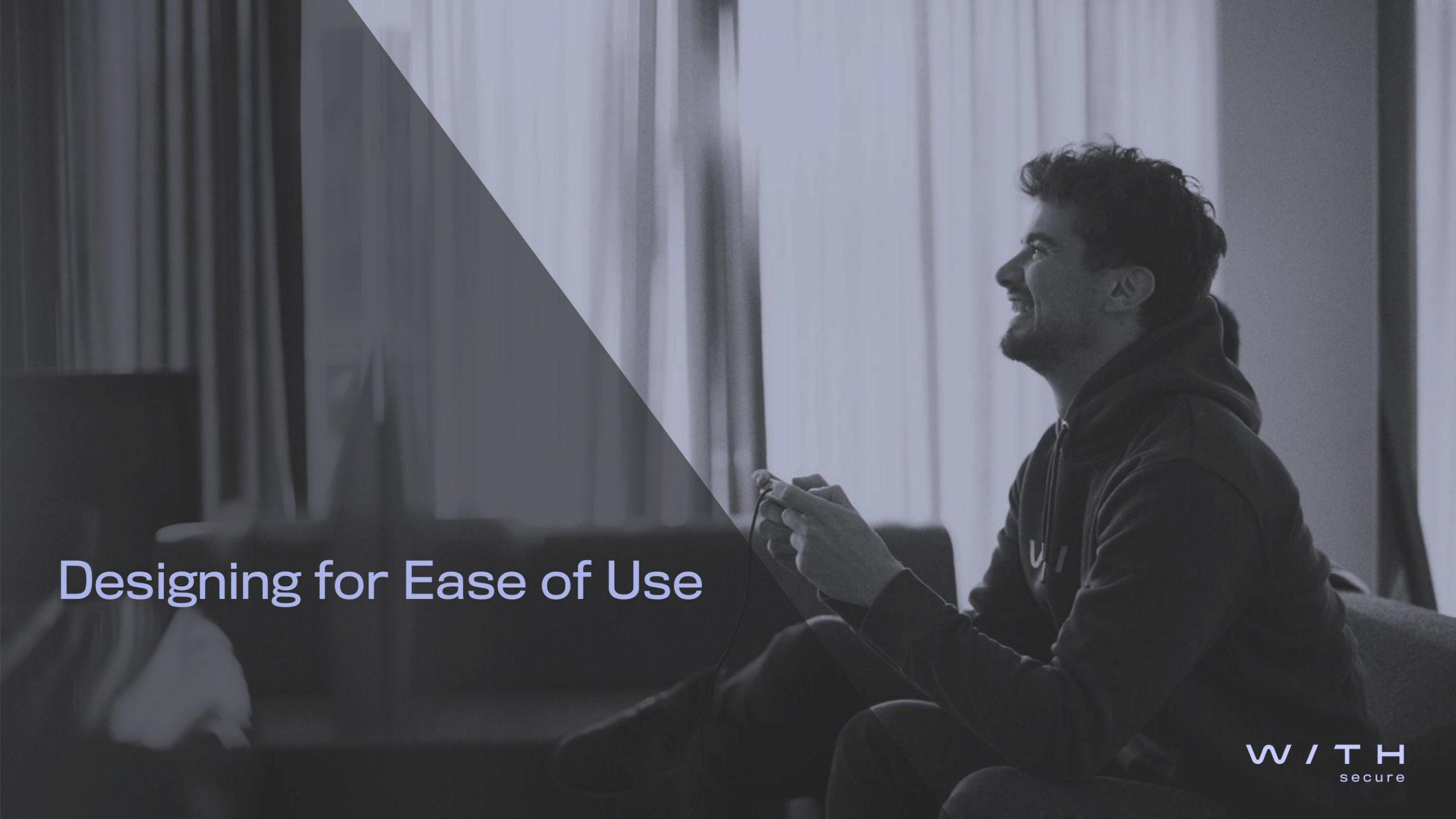

OFFLINE


VISITING ONLINE


OFFLINE


VISITING ONLINE


LIVING ONLINE



Designing for Ease of Use

WITH secure

1990s

Internet usage shifted from a specialized, technical audience to mainstream.

1990s

Internet usage shifted from a specialized, technical audience to mainstream.

1994

The first phishing tool, AOHell, was born

1990s

Internet usage shifted from a specialized, technical audience to mainstream.

1993

Repetitive work reduced via macro automation

Source: https://winworldpc.com/

1994

The first phishing tool, AOHell, was born

1990s

Internet usage shifted from a specialized, technical audience to mainstream.

1993

Repetitive work reduced via macro automation

Source: https://winworldpc.com/

1994

The first phishing tool, AOHell, was born

1995

The first macro virus, Virus:W32/Concept, was born

1990s

Internet usage shifted from a specialized, technical audience to mainstream.

1993

Repetitive work reduced via macro automation

1996

Email became free and revolutionized communication

Source: https://winworldpc.com/

Source: https://www.quora.com/

1994

The first phishing tool, AOHell, was born

1995

The first macro virus, Virus:W32/Concept, was born

1990s

Internet usage shifted from a specialized, technical audience to mainstream.

1993

Repetitive work reduced via macro automation

1996

Email became free and revolutionized communication

Source: https://winworldpc.com/

Source: https://www.quora.com/

1994

The first phishing tool, AOHell, was born

1995

The first macro virus, Virus:W32/Concept, was born

1999

The first email worm outbreak, Virus:W32/Melissa, occured

1998

Open-source code reduced enabled global collaboration and reduced re-invention

1998

Open-source code reduced enabled global collaboration and reduced re-invention

Late 2010’s

Rise of supply chain attacks via open-source libraries

1998

Open-source code reduced enabled global collaboration and reduced re-invention

1999

IEEE 802.11b brought WiFi to our living rooms

open source initiative

Late 2010's

Rise of supply chain attacks via open-source libraries

1998

Open-source code reduced enabled global collaboration and reduced re-invention

1999

IEEE 802.11b brought WiFi to our living rooms

open source initiative

Late 2010’s

Rise of supply chain attacks via open-source libraries

2008/2016

From router malware to IoT-based DDoS attacks

1998

Open-source code reduced enabled global collaboration and reduced re-invention

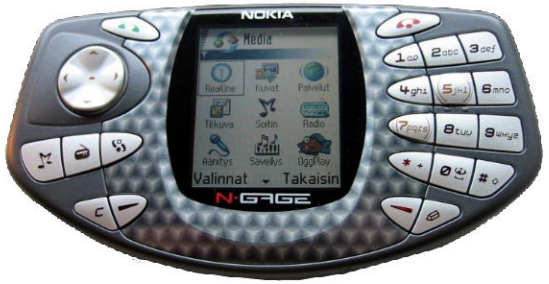
1999

IEEE 802.11b brought WiFi to our living rooms

2003

Symbian enabled us to carry applications at our fingertips

open source initiative



Late 2010's

Rise of supply chain attacks via open-source libraries

2008/2016

From router malware to IoT-based DDoS attacks

1998

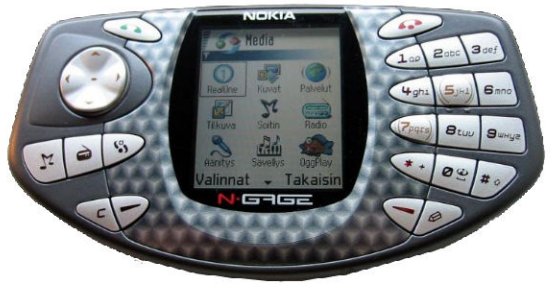
Open-source code reduced enabled global collaboration and reduced re-invention

1999

IEEE 802.11b brought WiFi to our living rooms

2003

Symbian enabled us to carry applications at our fingertips



Late 2010's

Rise of supply chain attacks via open-source libraries

2008/2016

From router malware to IoT-based DDoS attacks

2004

The first mobile phone worm, Bluetooth-Worm:SymbOS/Cabir was born

Rectifying the Misuse

Enforcement of long unique mixed-character passwords in websites and applications to prevent quick password cracking

Enforcement of long unique mixed-character passwords in websites and applications to prevent quick password cracking

Bruteforcing of strong passwords require GPU clusters and take longer to crack

Enforcement of long unique mixed-character passwords in websites and applications to prevent quick password cracking

Bruteforcing of strong passwords require GPU clusters and take longer to crack

Major browsers stopped supporting Adobe Flash Player due to popularity in Exploit Kits

Enforcement of long unique mixed-character passwords in websites and applications to prevent quick password cracking

Bruteforcing of strong passwords require GPU clusters and take longer to crack

Major browsers stopped supporting Adobe Flash Player due to popularity in Exploit Kits

Threat actors must hunt for other browser vulnerabilities to exploit

Enforcement of long unique mixed-character passwords in websites and applications to prevent quick password cracking

Bruteforcing of strong passwords require GPU clusters and take longer to crack

Major browsers stopped supporting Adobe Flash Player due to popularity in Exploit Kits

Threat actors must hunt for other browser vulnerabilities to exploit

Google deprecates and revokes overlay API in Android Q to address credential-stealing overlay-based applications

Enforcement of long unique mixed-character passwords in websites and applications to prevent quick password cracking

Bruteforcing of strong passwords require GPU clusters and take longer to crack

Major browsers stopped supporting Adobe Flash Player due to popularity in Exploit Kits

Threat actors must hunt for other browser vulnerabilities to exploit

Google deprecates and revokes overlay API in Android Q to address credential-stealing overlay-based applications

Threat actors would need Android's Accessibility Services (AAS) feature enabled and to do recon

Rebuilding for Ease of Use and Potential Misuse

WITH secure

Reduction of work credentials that needed to be remembered and secured.

Single Sign-On (SSO)

Reduction of work credentials that needed to be remembered and secured.

Single Sign-On (SSO)

Threat actors must find vulnerabilities to exploit in IAM providers

Reduction of work credentials that needed to be remembered and secured.

Application sandboxing was implemented to prevent apps from accessing other programs as well as critical system resources

Single Sign-On (SSO)

Threat actors must find vulnerabilities to exploit in IAM providers

Reduction of work credentials that needed to be remembered and secured.

Application sandboxing was implemented to prevent apps from accessing other programs as well as critical system resources

Single Sign-On (SSO)

Threat actors must find vulnerabilities to exploit in IAM providers

Threat actors must hunt for vulnerabilities to exploit to bypass sandboxes

Reduction of work credentials that needed to be remembered and secured.

Application sandboxing was implemented to prevent apps from accessing other programs as well as critical system resources

BitLocker feature was designed to provide encryption to protect devices that are lost or stolen

Single Sign-On (SSO)

Threat actors must find vulnerabilities to exploit in IAM providers

Threat actors must hunt for vulnerabilities to exploit to bypass sandboxes

Reduction of work credentials that needed to be remembered and secured.

Application sandboxing was implemented to prevent apps from accessing other programs as well as critical system resources

BitLocker feature was designed to provide encryption to protect devices that are lost or stolen

Single Sign-On (SSO)

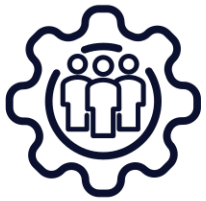
Threat actors must find vulnerabilities to exploit in IAM providers

Threat actors must hunt for vulnerabilities to exploit to bypass sandboxes

Threat actors must hunt for vulnerabilities to exploit to bypass BitLocker

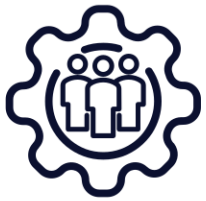
Learnings

People



A security mindset
Trained on users and misusers

People

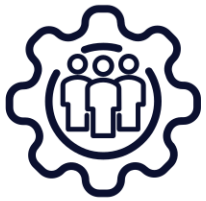


A security mindset
Trained on users and misusers

Processes

Built-in instead of bolt-on
Shifting responsibility left

People



A security mindset
Trained on users and misusers

Processes

Built-in instead of bolt-on
Shifting responsibility left

Technology

Shapes the security path
Resilient to human error
Designed for users and misusers

WITH®

secure