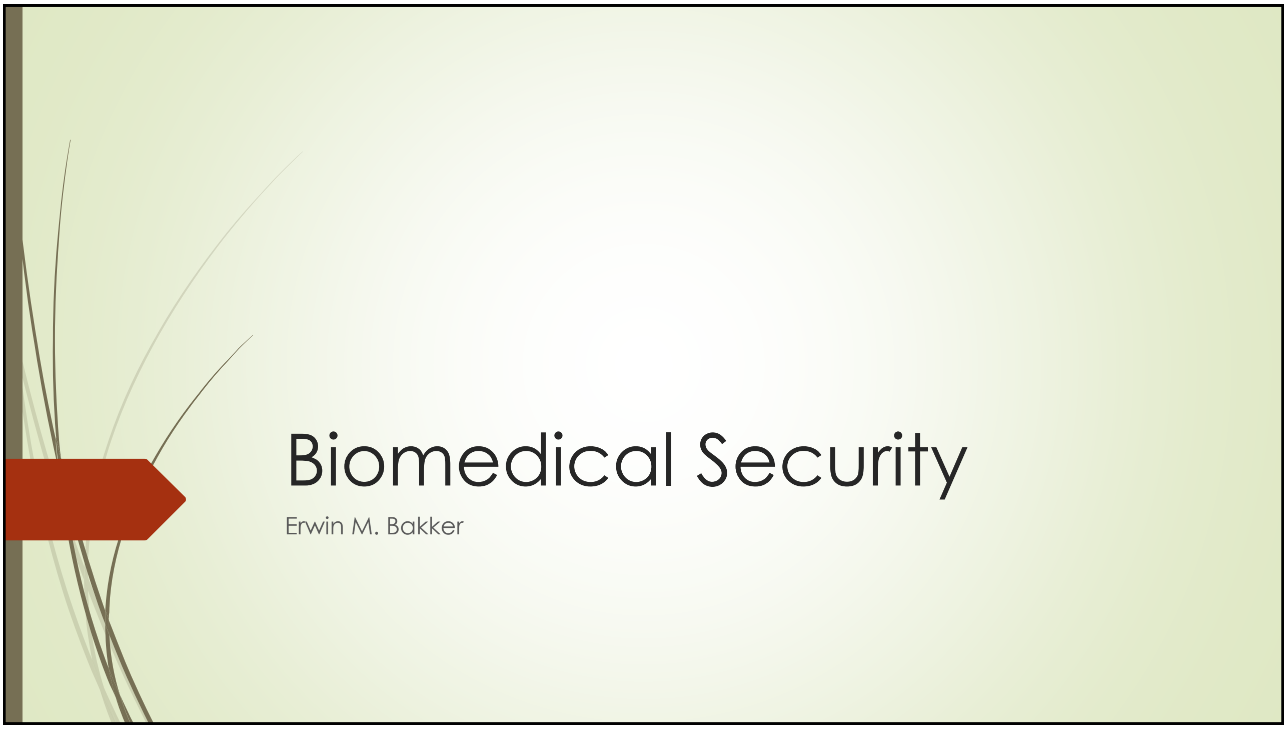
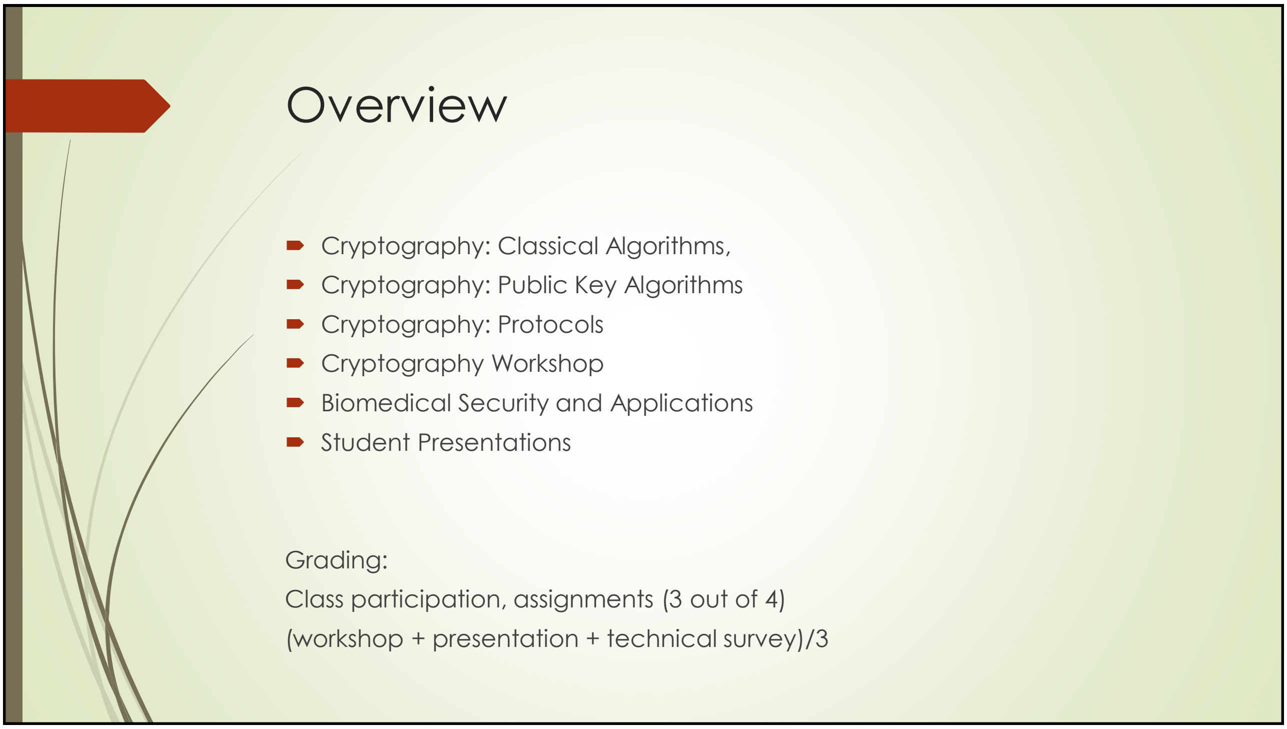


# Biomedical Security

Erwin M. Bakker



## Overview

- Cryptography: Classical Algorithms,
- Cryptography: Public Key Algorithms
- Cryptography: Protocols
- Cryptography Workshop
- Biomedical Security and Applications
- Student Presentations

Grading:
Class participation, assignments (3 out of 4)
(workshop + presentation + technical survey)/3

# Overview

- Cryptography: Classical Algorithms,
- Cryptography: Public Key Algorithms
- Cryptography: Protocols
- Cryptography Workshop
- Biomedical Security and Applications
- Student Presentations

Grading:

Class participation, assignments (3 out of 4) **All passed!**

(workshop + presentation + technical survey)/3

GGD regio Utrecht

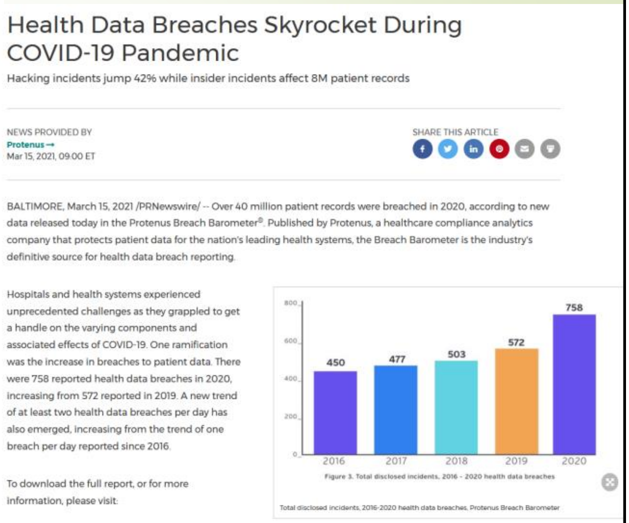
CORONAVACCINATIE: INFORMATIE OVER HET VACCINEREN

# Data of thousands of Dutch citizens leaked from government Covid-19 systems

Because of outdated systems and insufficient access control, almost all GGD employees had access to sensitive information, which has been illegally traded on the internet.

The data breach involves data from two GGD systems – CoronIT, which contains the private data of Dutch citizens who have taken a coronavirus test, and HPZone, an electronic file for source-and-contact research performed by the GGD. Addresses, telephone numbers, email addresses and citizen service numbers were accessed.

https://www.computerweekly.com/news/252495983/Data-of-thousands-of-Dutch-citizens-leaked-from-government-Covid-19-systems (Feb 2021).



Health Data Breaches Skyrocket During COVID-19 Pandemic

Hacking incidents jump 42% while insider incidents affect 8M patient records

NEWS PROVIDED BY
Protenus →
Mar 15, 2021, 09:00 ET

SHARE THIS ARTICLE

BALTIMORE, March 15, 2021 /PRNewswire/ -- Over 40 million patient records were breached in 2020, according to new data released today in the Protenus Breach Barometer®. Published by Protenus, a healthcare compliance analytics company that protects patient data for the nation's leading health systems, the Breach Barometer is the industry's definitive source for health data breach reporting.

Hospitals and health systems experienced unprecedented challenges as they grappled to get a handle on the varying components and associated effects of COVID-19. One ramification was the increase in breaches to patient data. There were 758 reported health data breaches in 2020, increasing from 572 reported in 2019. A new trend of at least two health data breaches per day has also emerged, increasing from the trend of one breach per day reported since 2016.

To download the full report, or for more information, please visit:

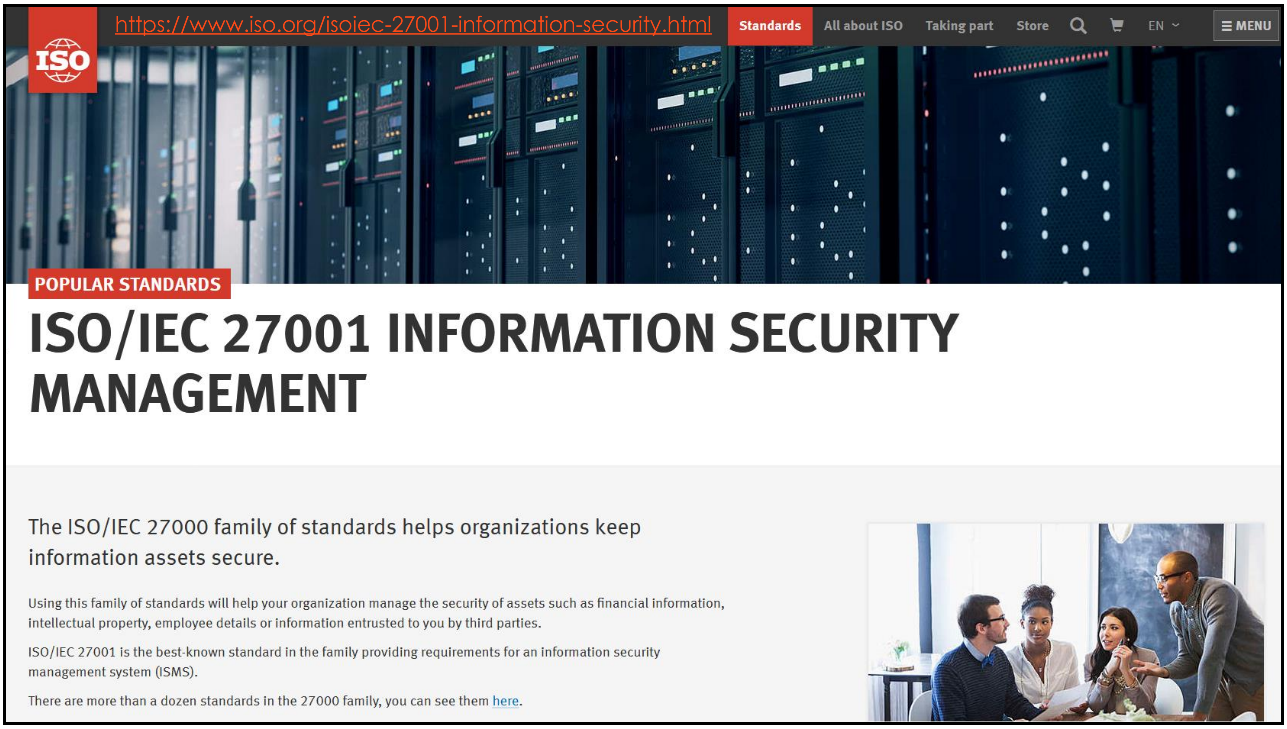
Figure 3. Total disclosed incidents, 2016 - 2020 health data breaches

Total disclosed incidents, 2016-2020 health data breaches, Protenus Breach Barometer

https://www.prnewswire.com/news-releases/health-data-breaches-skyrocket-during-covid-19-pandemic-301247097.html

## How to Secure Patient Data?

# Case: LUMC


https://www.iso.org/isoiec-27001-information-security.html

POPULAR STANDARDS

# ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT

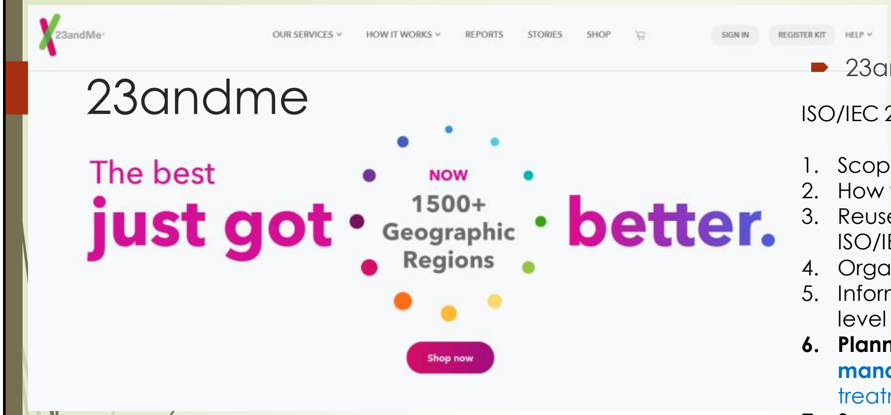
The ISO/IEC 27000 family of standards helps organizations keep information assets secure.

Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

There are more than a dozen standards in the 27000 family, you can see them here.

# 23andme



- 23andme.com ISO/IEC 27001

ISO/IEC 27001:2013 clauses and annex:

1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. **Planning an information security management system**; risk assessment; risk treatment
7. **Supporting** an information security management system
8. **Making** an information security management system **operational**
9. **Reviewing** the system's performance
10. **Corrective** action

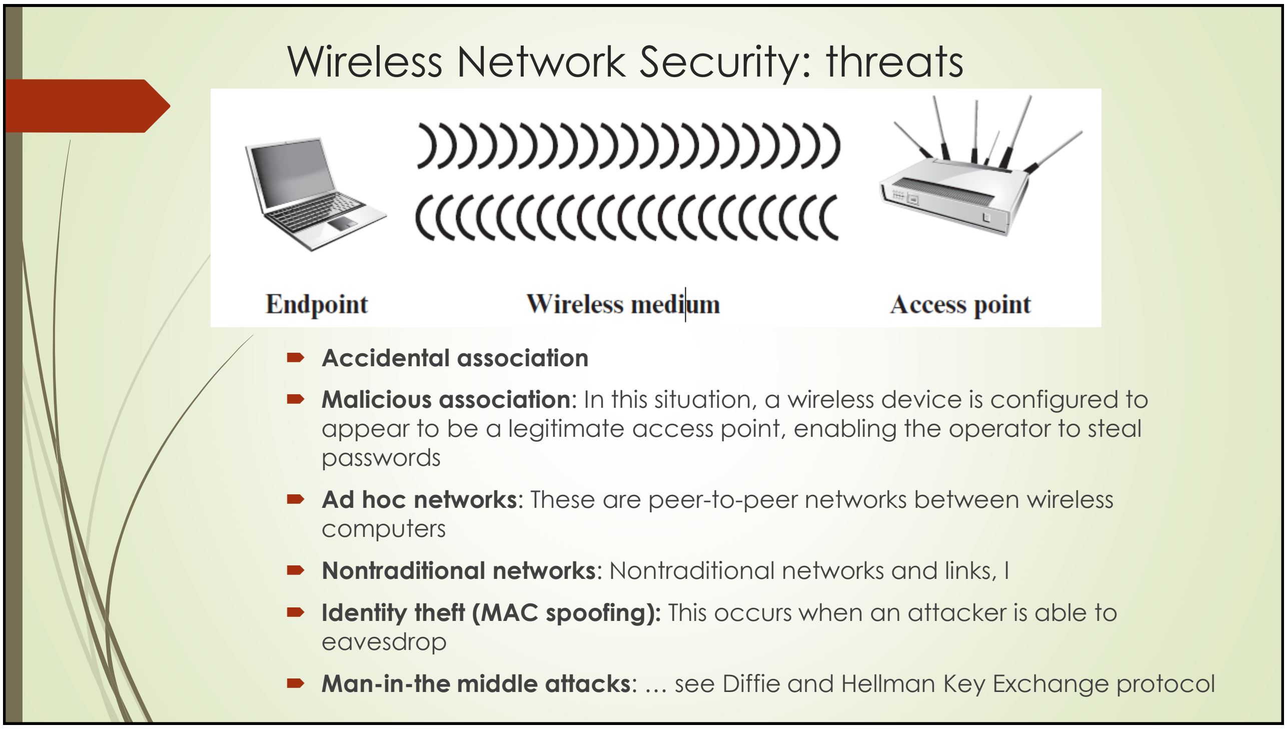
Annex A: List of controls and their objectives

Preventive, detective and corrective controls:

- **Physical controls** e.g. fences, doors, locks …
- **Procedural controls** e.g. incident response processes, training …
- **Technical controls** e.g. user authentication (login) and logical access controls, antivirus software, firewalls;
- **Legal and regulatory or compliance controls** e.g. privacy laws, policies and clauses.

# Wireless Network Security

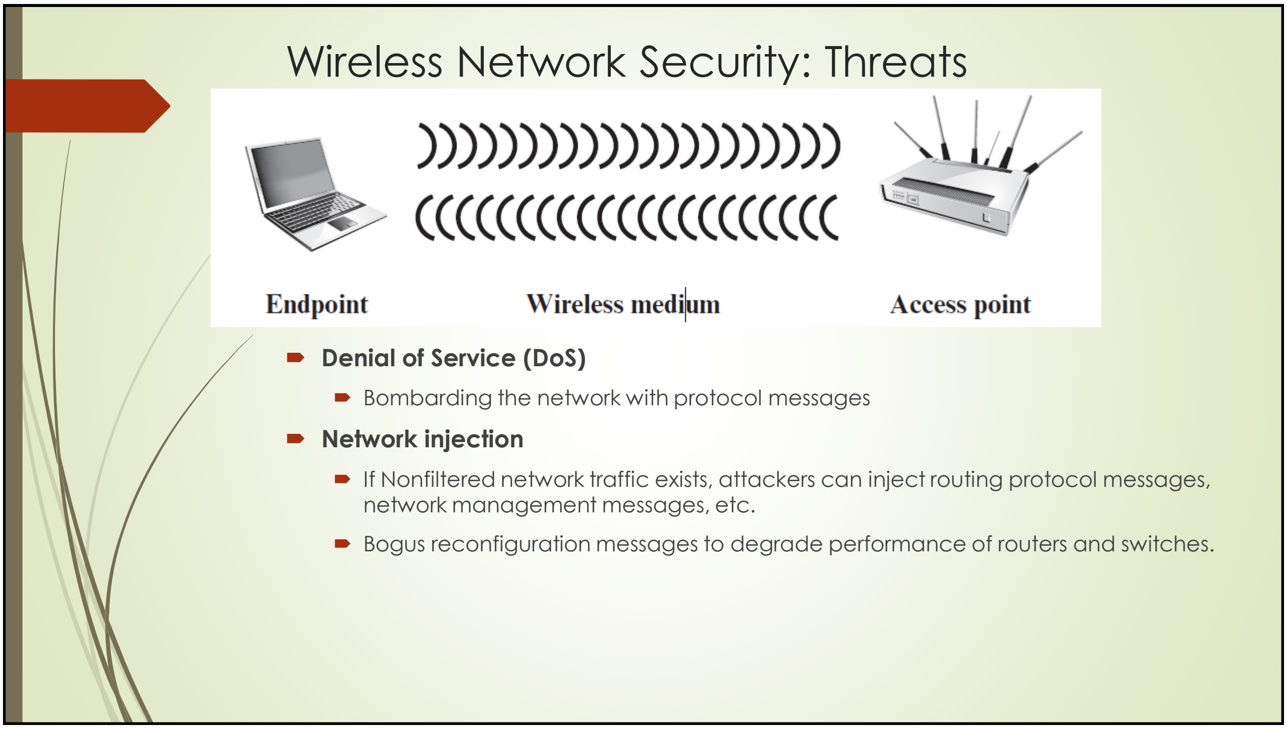
- Channel: broadcast communications
  - eavesdropping and jamming
  - active attacks that exploit vulnerabilities in communications protocols.
- Mobility
  - gives extra risks.
- Resources
  - Clients have often limited memory and processing resources with which to counter threats, including denial of service and malware.
- Accessibility
  - Wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations. This greatly increases their vulnerability to physical attacks.



## Wireless Network Security: threats

Endpoint
Wireless medium
Access point

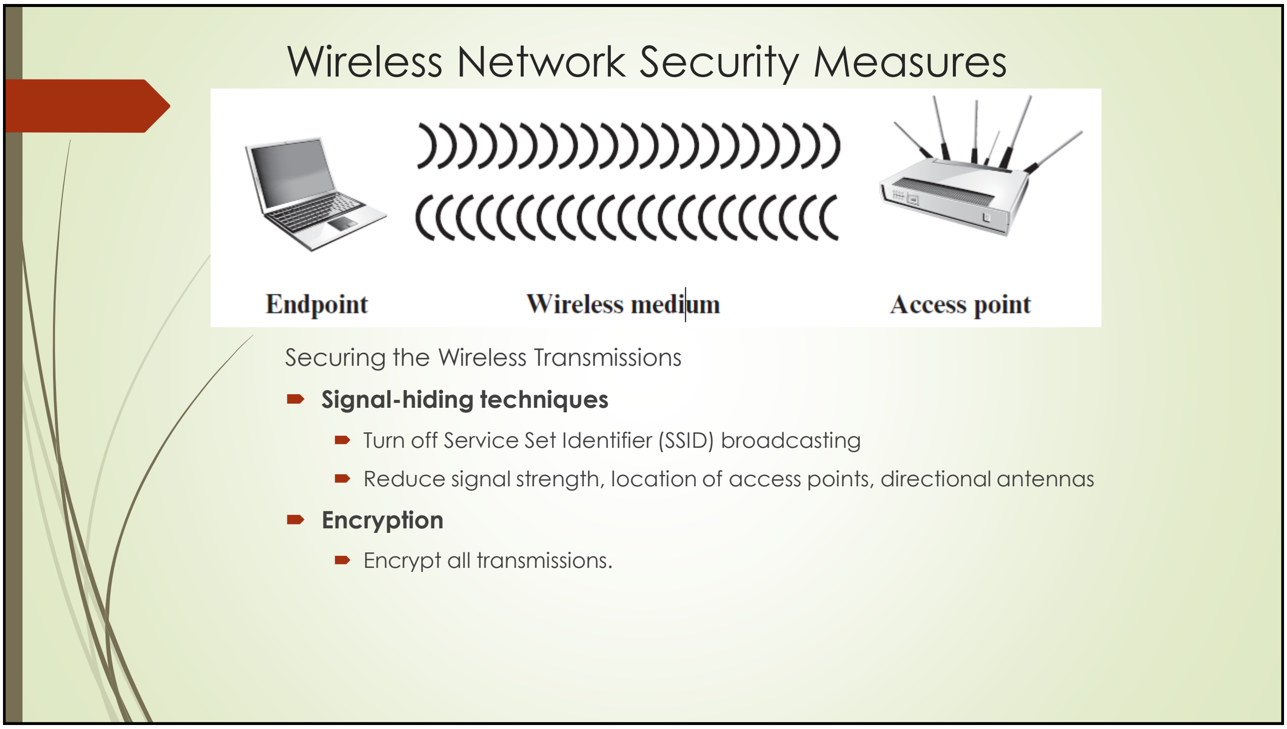
- **Accidental association**
- **Malicious association**: In this situation, a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords
- **Ad hoc networks**: These are peer-to-peer networks between wireless computers
- **Nontraditional networks**: Nontraditional networks and links, l
- **Identity theft (MAC spoofing):** This occurs when an attacker is able to eavesdrop
- **Man-in-the middle attacks**: … see Diffie and Hellman Key Exchange protocol



## Wireless Network Security: Threats

Endpoint
Wireless medium
Access point

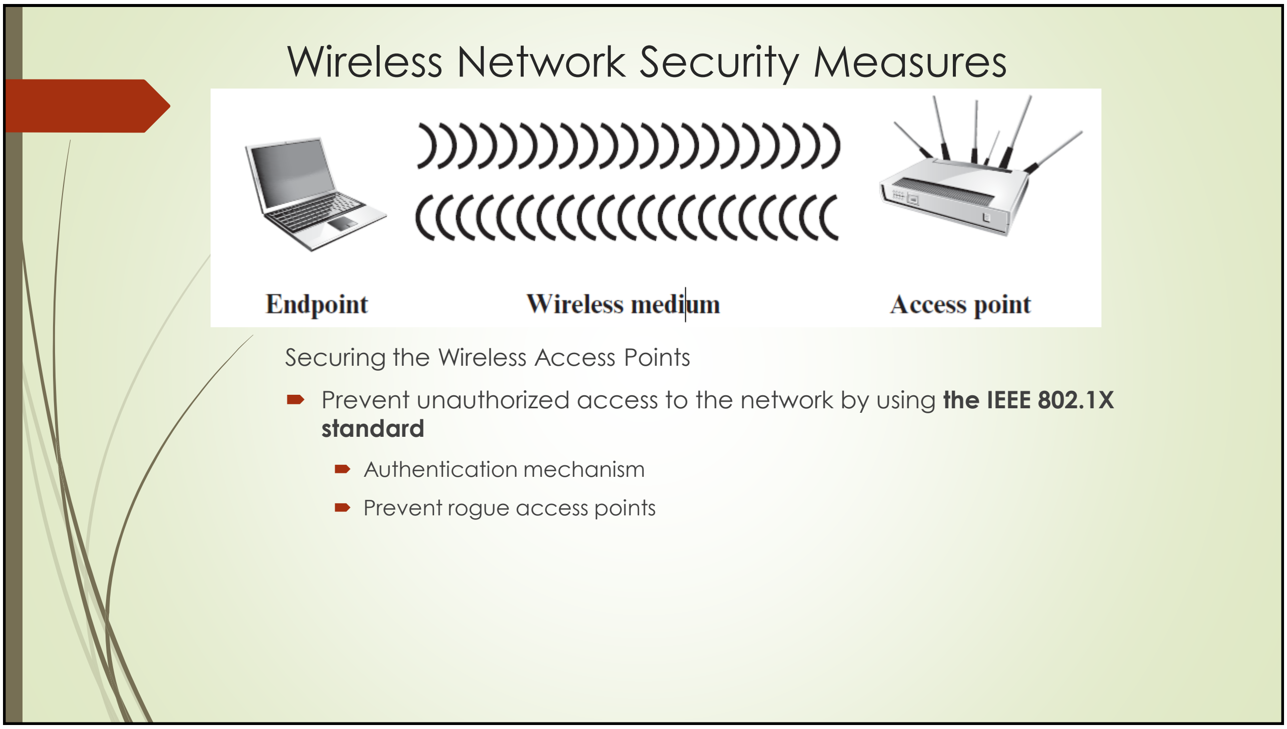
- **Denial of Service (DoS)**
  - Bombarding the network with protocol messages
- **Network injection**
  - If Nonfiltered network traffic exists, attackers can inject routing protocol messages, network management messages, etc.
  - Bogus reconfiguration messages to degrade performance of routers and switches.



# Wireless Network Security Measures

Securing the Wireless Transmissions

- **Signal-hiding techniques**
  - Turn off Service Set Identifier (SSID) broadcasting
  - Reduce signal strength, location of access points, directional antennas
- **Encryption**
  - Encrypt all transmissions.

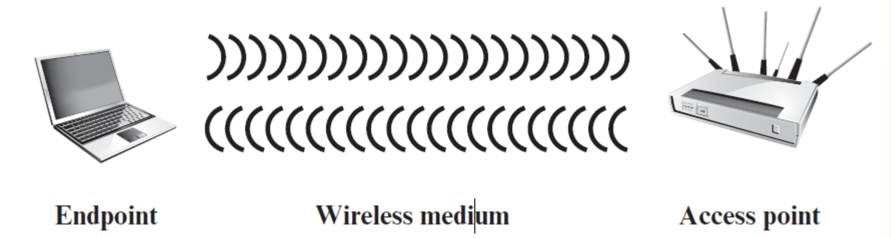


# Wireless Network Security Measures

Securing the Wireless Access Points

- Prevent unauthorized access to the network by using **the IEEE 802.1X standard**
  - Authentication mechanism
  - Prevent rogue access points

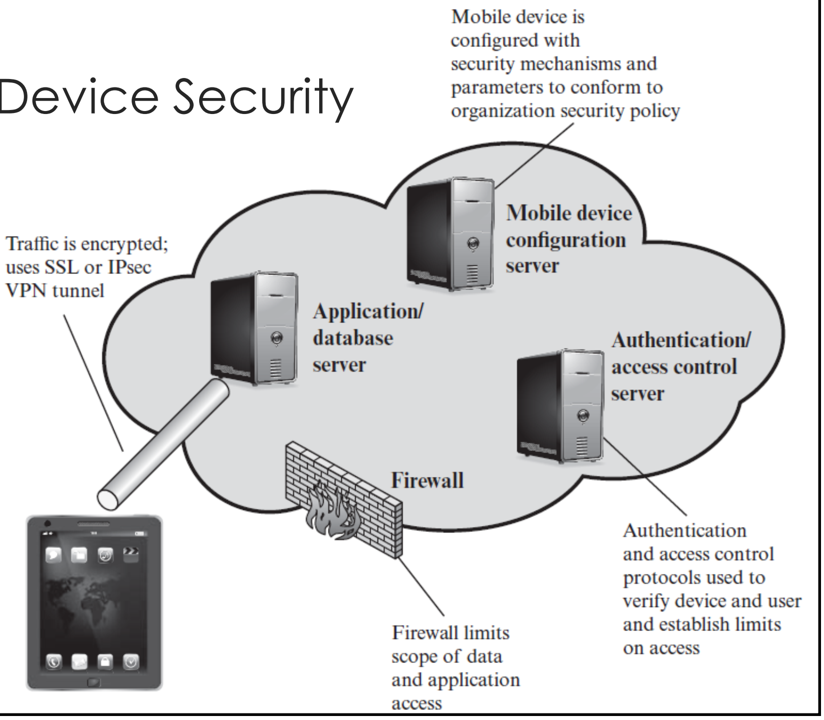
## Wireless Network Security Measures



Securing Wireless Networks

1. **Use encryption.** Wireless routers are typically equipped with built-in encryption mechanisms for router-to-router traffic.
2. **Use antivirus and antispyware software**, and a firewall on all wireless network endpoints.
3. **Turn off identifier broadcasting**. If a network is configured so that authorized devices know the identity of routers, this capability can be disabled, so as to thwart attackers.
4. **Change the identifier on your router from the default**. Again, this measure thwarts attackers who will attempt to gain access to a wireless network using default router identifiers.
5. **Change your router's pre-set password for administration**.
6. **Allow only specific computers to access your wireless** network. A router can be configured to only communicate with approved MAC addresses. Of course, MAC addresses can be spoofed, so this is just one element of a security strategy.

## Mobile Device Security


Mobile device configuration server
Application/ database server
Authentication/ access control server
Firewall

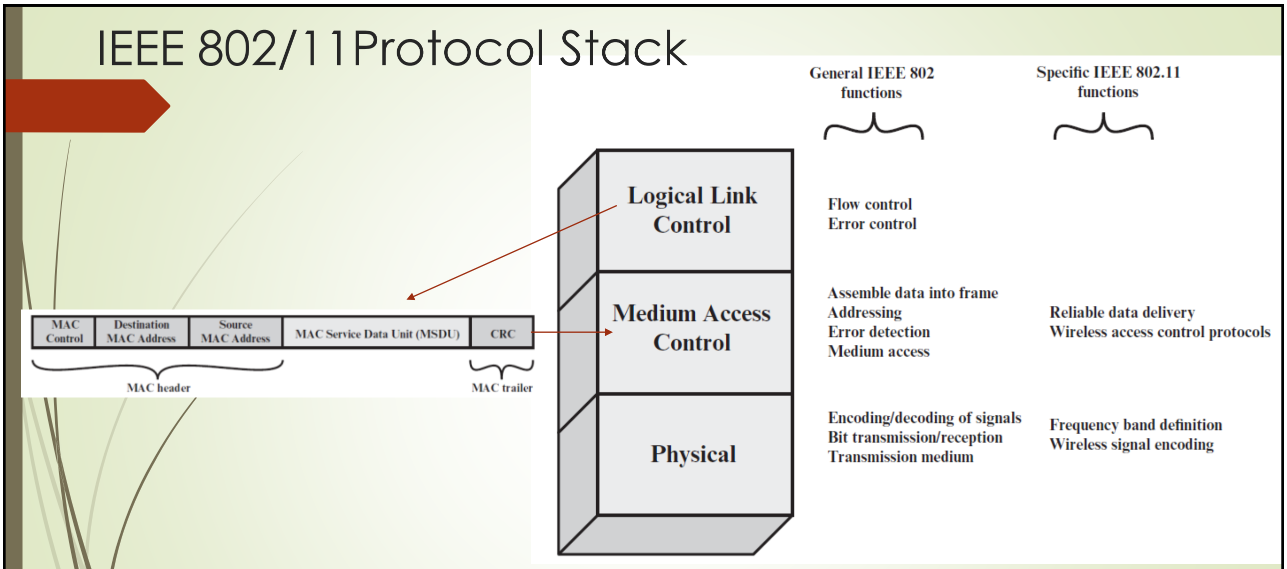
Mobile device is configured with security mechanisms and parameters to conform to organization security policy

Traffic is encrypted; uses SSL or IPsec VPN tunnel

Firewall limits scope of data and application access

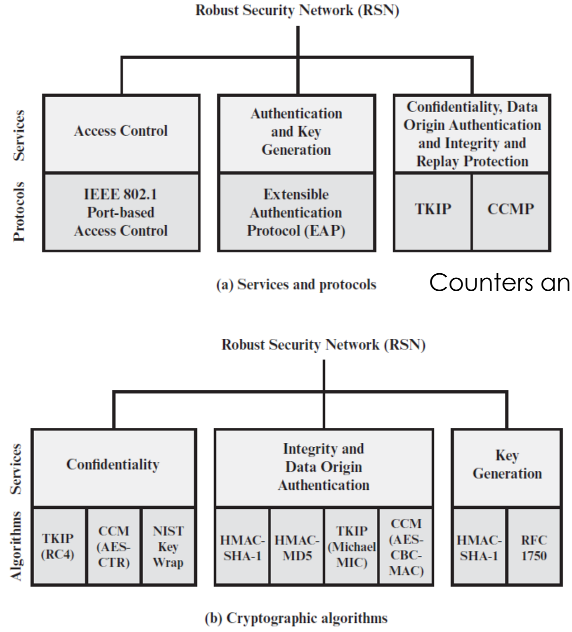
Authentication and access control protocols used to verify device and user and establish limits on access

# IEEE 802/11Protocol Stack



# The 802.11i RSN security specification

- **Authentication**: A protocol is used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.
- **Access control:** This function enforces the use of the authentication function, routes the messages properly, and facilitates key exchange. It can work with a variety of authentication protocols.
- **Privacy with message integrity**: MAC-level data (e.g., an LLC PDU) are encrypted along with


Robust Security Network (RSN)
Services
Protocols
Access Control
Authentication and Key Generation
Confidentiality, Data Origin Authentication and Integrity and Replay Protection
IEEE 802.1 Port-based Access Control
Extensible Authentication Protocol (EAP)
TKIP
CCMP
(a) Services and protocols
Robust Security Network (RSN)
Services
Algorithms
Confidentiality
Integrity and Data Origin Authentication
Key Generation
TKIP (RC4)
CCM (AES-CTR)
NIST Key Wrap
HMAC-SHA-1
HMAC-MD5
TKIP (Michael MIC)
CCM (AES-CBC-MAC)
HMAC-SHA-1
RFC 1750
(b) Cryptographic algorithms

CBC-MAC = Cipher Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

Counters and Block Chaining

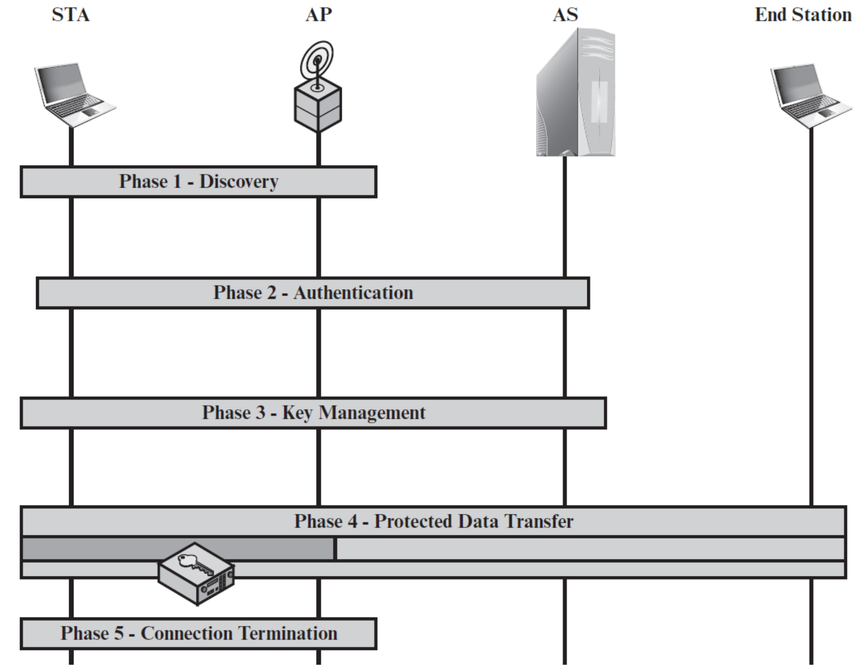
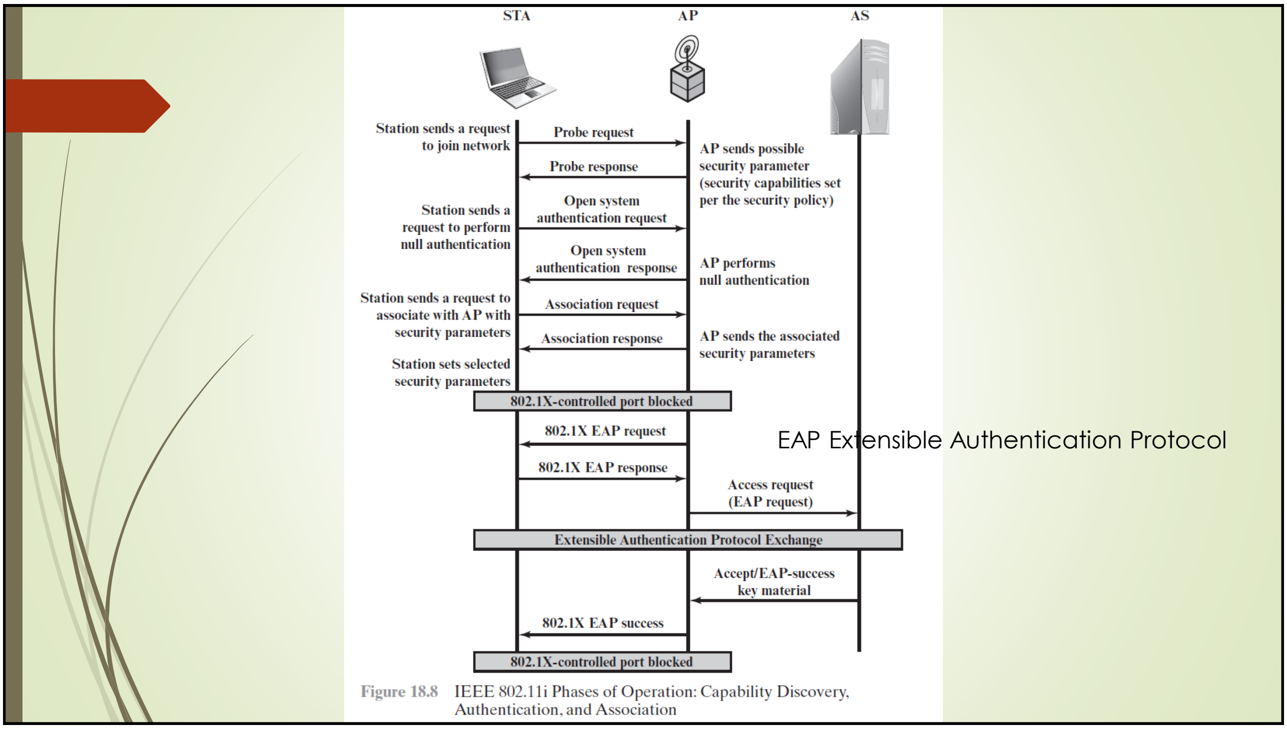


Figure 18.7 IEEE 802.11i Phases of Operation



STA
AP
AS

Station sends a request to join network

Probe request

Probe response

AP sends possible security parameter (security capabilities set per the security policy)

Station sends a request to perform null authentication

Open system authentication request

Open system authentication response

AP performs null authentication

Station sends a request to associate with AP with security parameters

Association request

Association response

AP sends the associated security parameters

Station sets selected security parameters

802.1X-controlled port blocked

802.1X EAP request

802.1X EAP response

Access request (EAP request)

Extensible Authentication Protocol Exchange

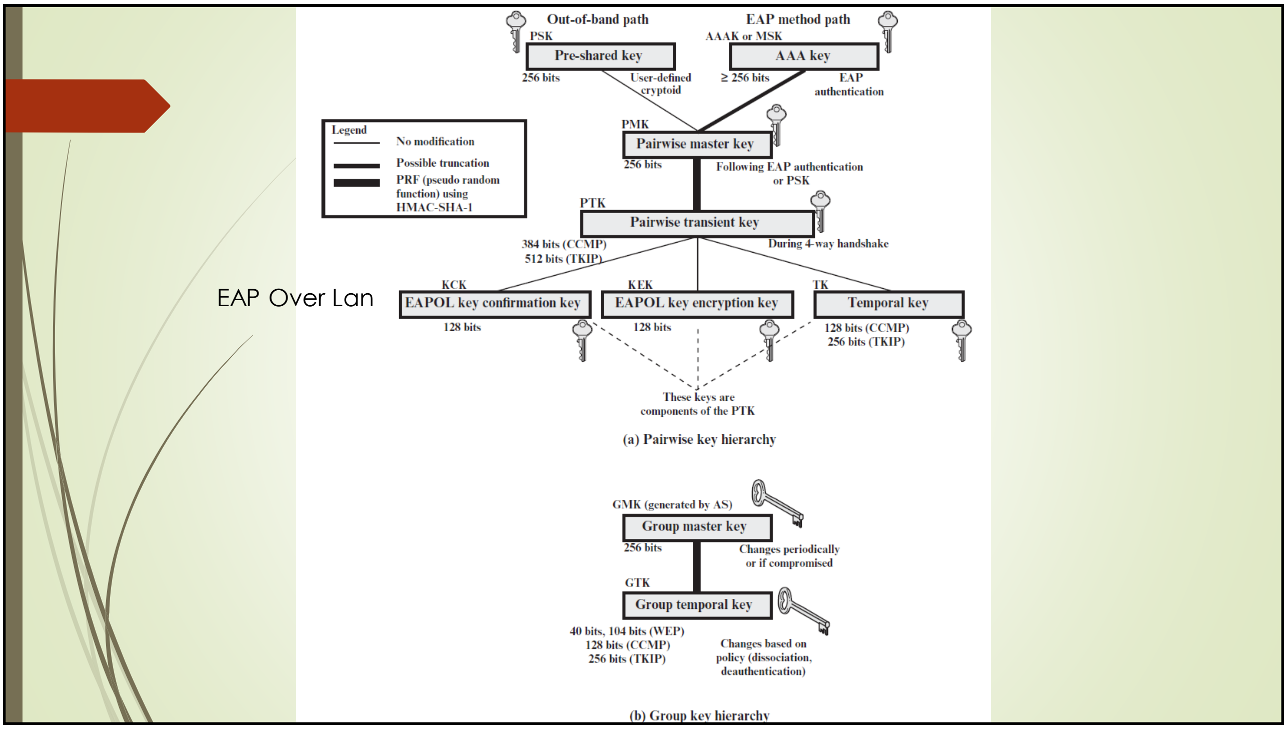
Accept/EAP-success key material

802.1X EAP success

802.1X-controlled port blocked

Figure 18.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association

EAP Extensible Authentication Protocol



Out-of-band path

PSK
Pre-shared key
256 bits
User-defined cryptoid

EAP method path

AAAK or MSK
AAA key
≥ 256 bits
EAP authentication

Legend
No modification
Possible truncation
PRF (pseudo random function) using HMAC-SHA-1

PMK
Pairwise master key
256 bits
Following EAP authentication or PSK

PTK
Pairwise transient key
384 bits (CCMP)
512 bits (TKIP)
During 4-way handshake

KCK
EAPOL key confirmation key
128 bits

KEK
EAPOL key encryption key
128 bits

TK
Temporal key
128 bits (CCMP)
256 bits (TKIP)

These keys are components of the PTK

(a) Pairwise key hierarchy

GMK (generated by AS)
Group master key
256 bits
Changes periodically or if compromised

GTK
Group temporal key
40 bits, 104 bits (WEP)
128 bits (CCMP)
256 bits (TKIP)
Changes based on policy (dissociation, deauthentication)

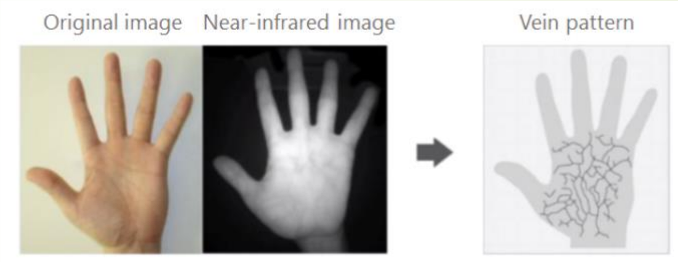
(b) Group key hierarchy

EAP Over Lan

# Biometrics Security

Security based on

- Fingerprints,
- Retina scans
- Face recognition
- Voice recognition
- Gait analysis
- EEG scan
- DNA
- …



Forensics

A good idea?

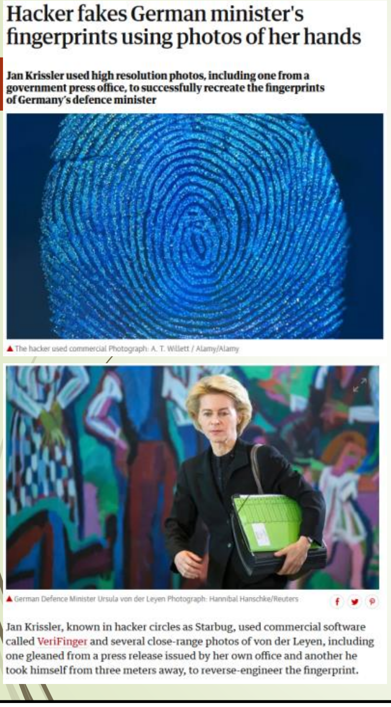
80,406 views | Aug 14, 2019, 04:31am

## New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report

Zak Doffman Contributor ⓘ
Cybersecurity
*I write about security and surveillance.*

GETTY

https://www.forbes.com



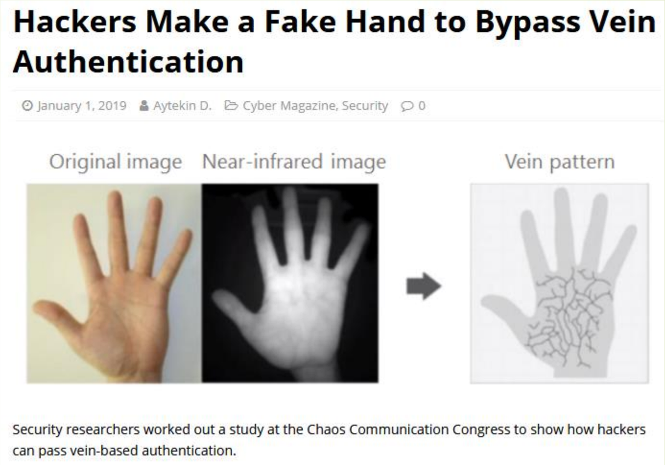
## Hacker fakes German minister's fingerprints using photos of her hands

**Jan Krissler used high resolution photos, including one from a government press office, to successfully recreate the fingerprints of Germany's defence minister**

▲ The hacker used commercial Photograph: A. T. Willett / Alamy/Alamy

▲ German Defence Minister Ursula von der Leyen Photograph: Hannibal Hanschke/Reuters

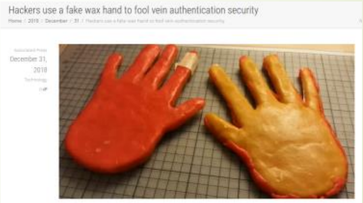
Jan Krissler, known in hacker circles as Starbug, used commercial software called VeriFinger and several close-range photos of von der Leyen, including one gleaned from a press release issued by her own office and another he took himself from three meters away, to reverse-engineer the fingerprint.



## Hackers Make a Fake Hand to Bypass Vein Authentication

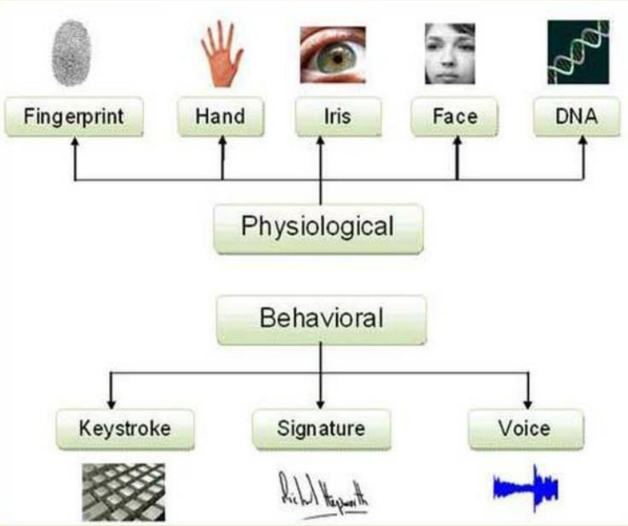
January 1, 2019 Aytekin D. Cyber Magazine, Security 0

Security researchers worked out a study at the Chaos Communication Congress to show how hackers can pass vein-based authentication.

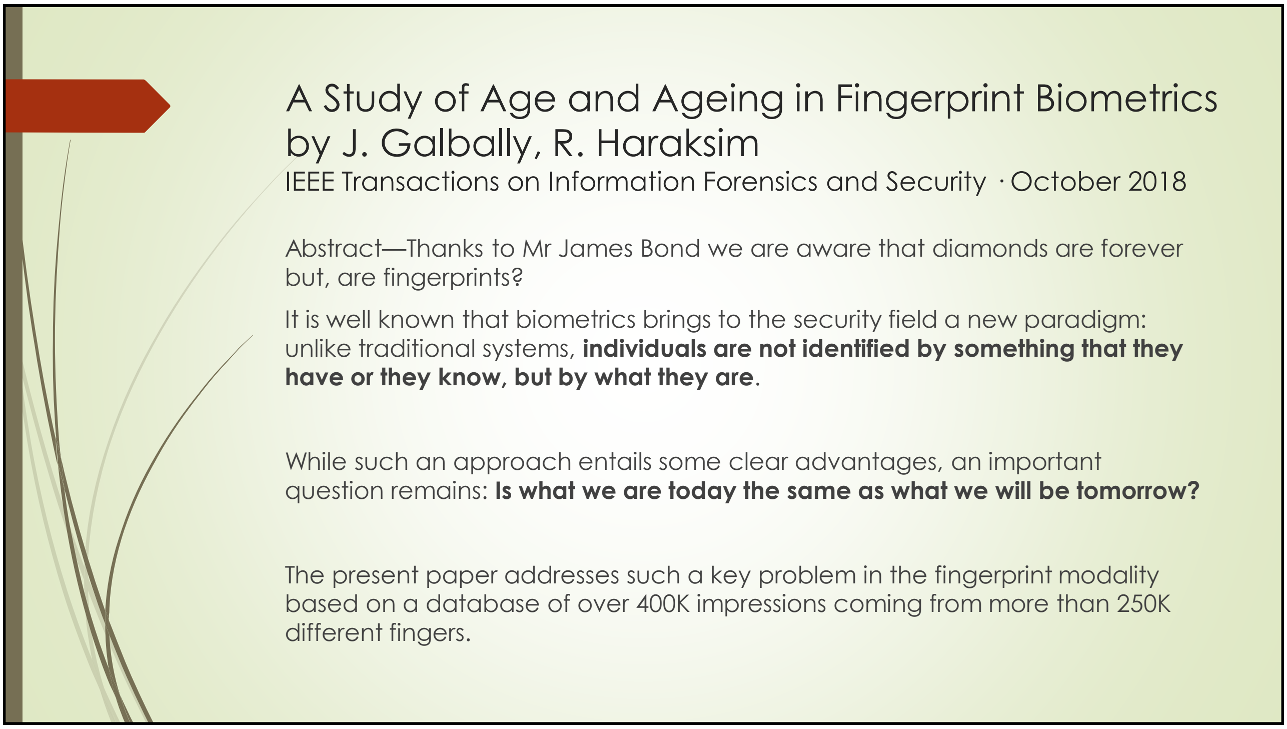


Hackers use a fake wax hand to fool vein authentication security

December 31, 2018



T.Sabhanayagam, V. Prasanna Venkatesan, K. Senthamaraikannan, A Comprehensive Survey on Various Biometric Systems International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2276-2297 © Research India Publications. http://www.ripublication.com



## A Study of Age and Ageing in Fingerprint Biometrics by J. Galbally, R. Haraksim

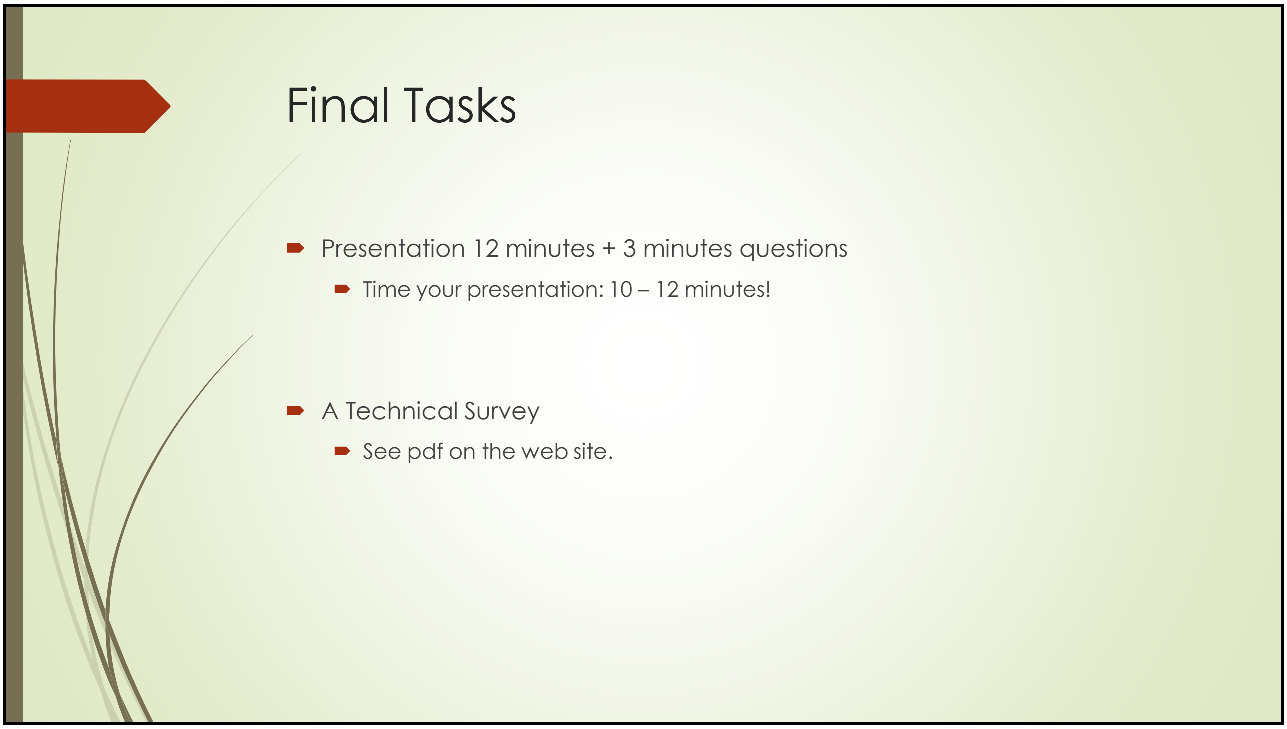
IEEE Transactions on Information Forensics and Security · October 2018

Abstract—Thanks to Mr James Bond we are aware that diamonds are forever but, are fingerprints?

It is well known that biometrics brings to the security field a new paradigm: unlike traditional systems, **individuals are not identified by something that they have or they know, but by what they are**.

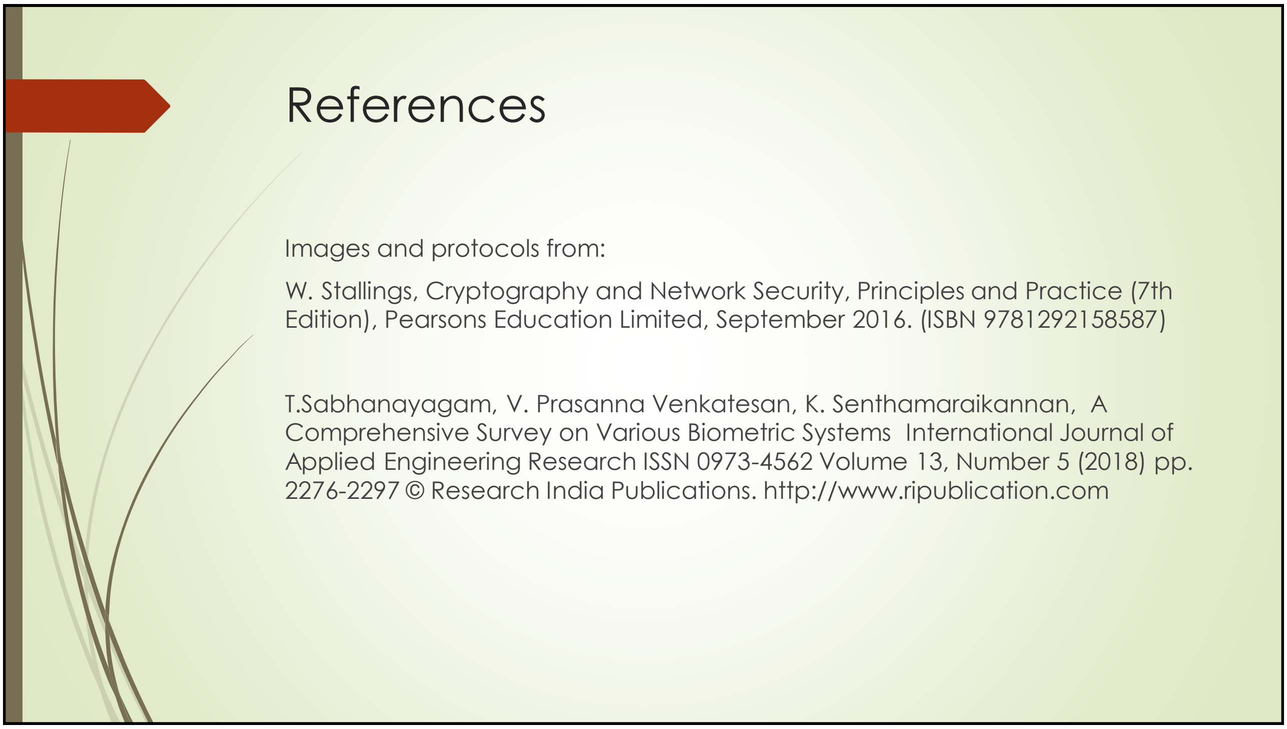
While such an approach entails some clear advantages, an important question remains: **Is what we are today the same as what we will be tomorrow?**

The present paper addresses such a key problem in the fingerprint modality based on a database of over 400K impressions coming from more than 250K different fingers.



## Final Tasks

- Presentation 12 minutes + 3 minutes questions
  - Time your presentation: 10 – 12 minutes!
- A Technical Survey
  - See pdf on the web site.



# References

Images and protocols from:

W. Stallings, Cryptography and Network Security, Principles and Practice (7th Edition), Pearsons Education Limited, September 2016. (ISBN 9781292158587)

T.Sabhanayagam, V. Prasanna Venkatesan, K. Senthamaraikannan, A Comprehensive Survey on Various Biometric Systems International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2276-2297 © Research India Publications. http://www.ripublication.com