Zero Trust Security (ZTS) Model

CYBR371: System and Network Security, (2024/T1)

Arman Khouzani, Mohammad Nekooei
Slides modified from "Masood Mansoori"

19 May 2024

Victoria University of Wellington – School of Engineering and Computer Science

Agenda

Perimeter Security

ZTS: Key Principles

ZTS: Core Components

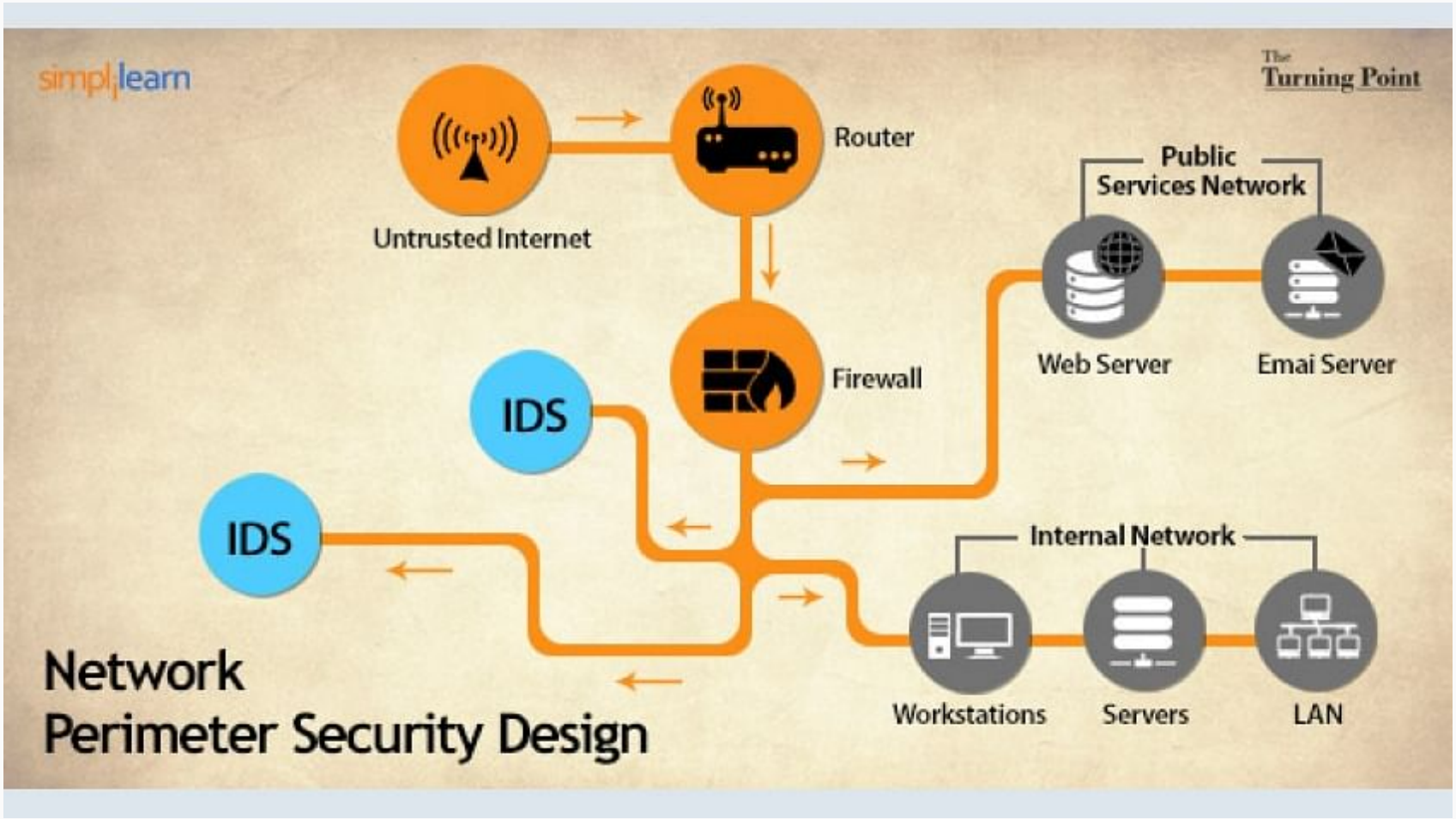
Implementation Challenges

ZTS: Benefits

Perimeter Security

Classical Approach: Security "Perimeter"

Traditionally (good'ol days!), enterprise security was based on creating a security **perimeter**, a.k.a. "*castle-and-moat*" model:



Ref: https://www.simplilearn.com/network-perimeter-security-design-article

Security “Perimeter” (Classical Approach)

Perimeter security: creating a strong, defined boundary around a network or system to keep out potential threats (implicitly, assuming a higher trust within the perimeter).

This was achieved using:

- Secure gateways
- Firewalls
- NIDS/NIDPS
- centrally configured endpoints, using e.g. “Group Policy Objects (GPO)” in Windows networks, or “Puppet”/“Chef” in Linux networks.
- centrally configured accounts and permissions, using e.g. “Active Directory (AD)” in Windows networks or “Kerberos”/“openLDAP” in Linux networks.

Perimeter Security Design: Main Characteristics

- strong perimeter defence
- trust by location (once a user or device was inside the perimeter, it was generally assumed to be trustworthy).
- single (or few) point(s) of entry (making it easier to monitor and control access).
- static security measures (e.g. fixed firewall rules and access control lists).
- minimal internal segmentation.
- focus on external threats
- limited visibility and control of internal activities (instead, relied heavily on monitoring the perimeter)
- simplified user access
- point solutions (addressing specific threats without integrating with other security measures)

Perimeter Security: Context

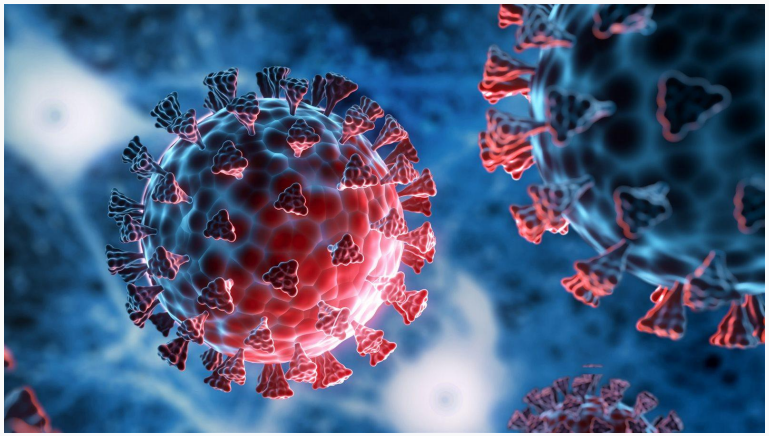
This worked relatively fine because:

- There were few clear points of entry and exit (ingress and egress) for network traffic to an organisation.
- The network of an organisation was typically contained and had a well-defined perimeter.
- Most employees worked on-premises, and access to internal resources from outside the organisation was rare.
- IT environments were more uniform (fewer types of devices/platforms), hence easier to secure the perimeter.
- Cyber-threats were less sophisticated, and attacks were generally less frequent and less complex.
- Data and applications were typically hosted on internal servers within the network perimeter.

Security Perimeter: So, what changed?!

Changes that made perimeter security less desirable:

- Increased Remote Work



Security Perimeter: So, what changed?!

- Cloud Adoption
- Mobile Devices& BYOD
- Sophisticated Cyber Threats
- Increased Interconnectivity (partners, suppliers, tenants, customers)
- Regulatory requirements (e.g. GDPR, CCPA, PCI-DSS) demands stricter access control and detailed monitoring.
- IoT/OT

There were also inherent problems:

- flat network architecture meant ease of *lateral movement*.
- neglected/downplayed the risk of insider threat.

The need for a new approach

- Granular Access Control
- Continuous Verification (of the identity and integrity of users and devices).
- **Micro-Segmentation**: to minimise the blast radius.
- Adaptive Security (adapting to changing conditions and threats, using real-time data and analytics to adjust security policies dynamically)
- Enhanced Visibility
- Cloud and Remote Work Support

What is Zero Trust?

Zero Trust: "Never Trust, Always Verify."

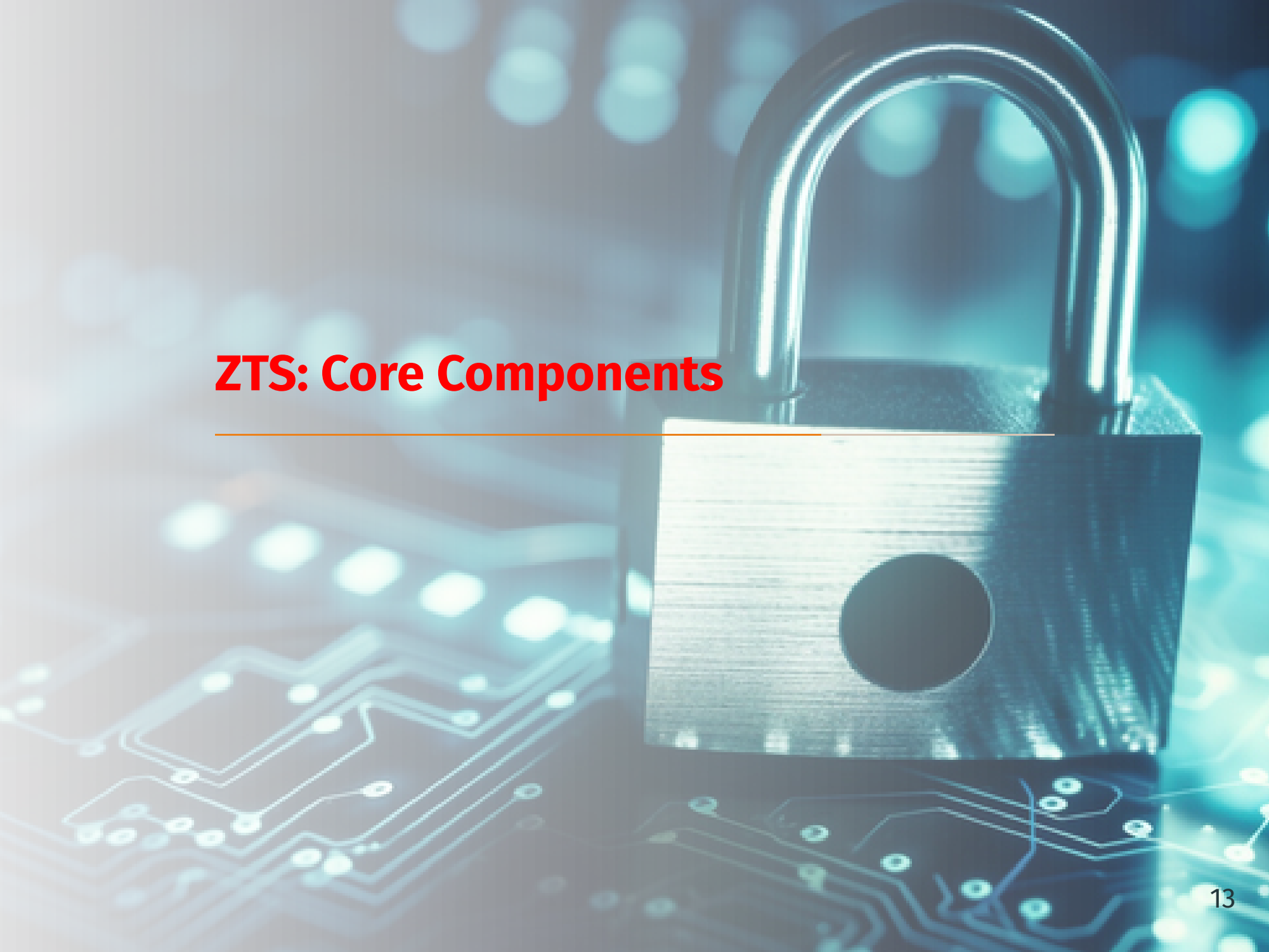
- Security model that assumes no entity, inside or outside the network, should be trusted by default.
- Every access request must be verified, regardless of origin.

ZTS: Key Principles

Key Principles of Zero Trust

- **Verify Explicitly:** Authenticate and authorise every access request.
- **Use Least Privilege Access:** Limit access to necessary resources.
- **Assume Breach:** Design security strategies assuming a breach.

ZTS: Core Components



Core Components of Zero Trust Architecture

- **Identity and Access Management (IAM):** Ensures authenticated and authorised access.
- **Multi-Factor Authentication (MFA):** Requires multiple forms of verification.
- **Network Segmentation:** Isolates network segments to prevent lateral movement.
- **Endpoint Security:** Monitors and protects devices accessing the network.
- **Data Encryption:** Protects data at rest and in transit.
- **Continuous Monitoring and Analytics:** Detects and responds to anomalies.

Implementation Challenges

Implementation Challenges

- **Complexity:** Requires changes to infrastructure and processes.
- **Cost:** Significant upfront costs for tools and technologies.
- **Cultural Shift:** Emphasises continuous verification over implicit trust.

ZTS: Benefits

Benefits of Zero Trust

- **Improved Security:** Reduces risk of unauthorised access and breaches.
- **Enhanced Visibility:** Better insight into user activities and network traffic.
- **Regulatory Compliance:** Helps meet data protection and security requirements.

Next: Cloud/IoT Security