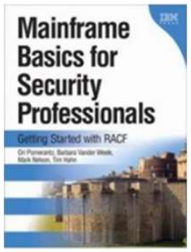
Zero Trust and RACF®

Moving Towards Least Access Privilege

Mark Nelson, CISSP®, CSSLP®
IBM® Poughkeepsie

November 2024



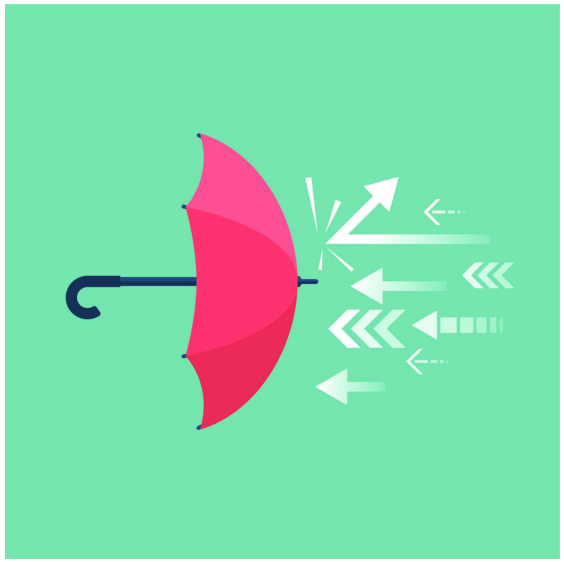
What is “Zero Trust” and “Why do I Care”?

Is Zero Trust:

…. The single most important step forward in security architecture that will revolutionize how we protect our systems

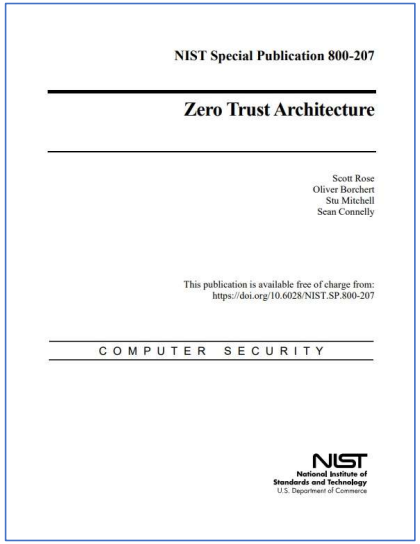
- or –

… Yet another scam initiated by organizations who know nothing about security in the real world, designed to scare our management into buying products to address a problem which doesn’t really exist?



Zero Trust: Let's Go to the Source

- **National Institute of Standards and Technology (NIST) Special Publication 800-207 is considered by many to be the foundation for Zero Trust discussions**
- **It defines the Zero Trust (ZT) model and its principles and the Zero Trust Architecture (ZTA) that is built on the Zero Trust model.**


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

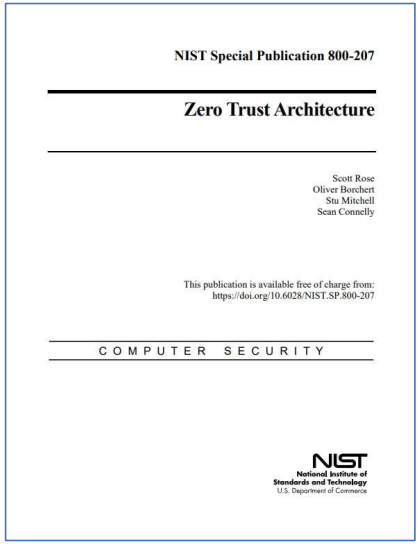
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Zero Trust: Let's Go to the Source…

- "**ZT is** not a single architecture but **a set of guiding principles for workflow, system design and operations** that can be used to improve the security posture of any classification or sensitivity level" (p.1)
- "**Transitioning to ZTA is a journey** concerning how an organization evaluates risk in its mission **and cannot simply be accomplished with a wholesale replacement of technology"** (p.1)
- **"Zero Trust (ZT)** provides a **collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege** per-request access decisions in information systems and services in the face of a network viewed as compromised" (p.4).


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Zero Trust: Let's Go to the Source…

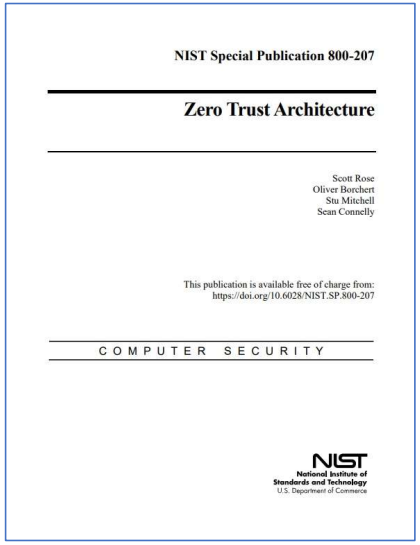
- **What are the tenets of Zero Trust? (p.6 and 7)**

  1. "All data sources and computing services are considered resources"

  2. "All Communication is secure regardless of network location"

  3. "Access to individual enterprise resources is granted on per session basis"

  4. "Access to resources is determined by dynamic policy, including the observable state of client identity, application/service and the requesting asset – and may include other behavioral and environmental attributes"


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

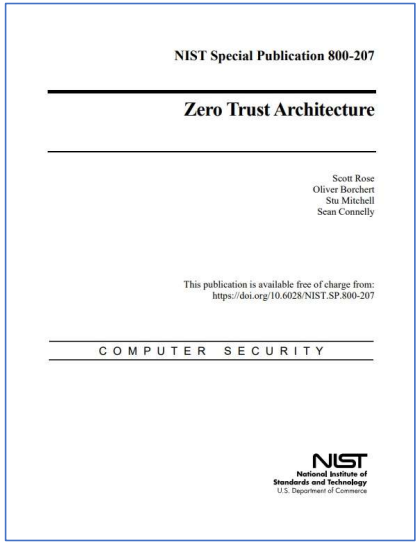
Zero Trust: Let's Go to the Source…

- **What are the tenets of Zero Trust? (p.6 and 7)…**

5. "The enterprise monitors and measures the integrity and security posture of all owned and associated assets."

6. "All resource authentication and authorization are dynamic and strictly enforced before access is allowed. "

7. "The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. "


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Is Zero Trust Really All That New?

Is Zero Trust all that new or is it an application of generally accepted security principles?

The “Fundamental Principles “ of Security

- **Least Privilege**
  - Each system component or process should have the least authority necessary to perform its duties
- **Separation of Duties**
  - At least two individuals are responsible for the completion of a task
- **Defense in Depth**
  - The practice of arranging defensive lines or fortifications so that they can defend each other, especially in case of an enemy incursion
- **Fail Securely**
  - A failure will cause no harm or at least a minimum of harm to other devices or danger to personnel, and doesn't cause the system to be insecure
- **Establish Secure Defaults**
  - The default configuration settings are the most secure settings possible, which are not necessarily the most user-friendly settings
- **Minimize the Attack Surface**
  - “A chain is only as strong as its weakest link”
  - Keep security simple

What About the “Fundamental Principles “ of Security?

They all apply!

- **Least Privilege** 
  - Each system component or process should have the least authority necessary to perform its duties
- **Separation of Duties** 
  - At least two individuals are responsible for the completion of a task
- **Defense in Depth** 
  - The practice of arranging defensive lines or fortifications so that they can defend each other, especially in case of an enemy incursion
- **Fail Securely** 
  - A failure will cause no harm or at least a minimum of harm to other devices or danger to personnel, and doesn't cause the system to be insecure
- **Establish Secure Defaults** 
  - The default configuration settings are the most secure settings possible, which are not necessarily the most user-friendly settings
- **Minimize the Attack Surface** 
  - “A chain is only as strong as its weakest link”
  - Keep security simple

ZT: It’s Not Just About Information Technology

- When my grandmother was in her late 80s/early 90s, she was living at home alone.
- One afternoon, two men appeared at her door wearing construction uniforms, hard hats and carrying clip boards, claiming to be from the water company there to “investigate a water problem”.
- She let them in and as one was with her in her basement looking at pipes, the other was upstairs stealing valuables.

(Not my actual grandmother)

Let’s Look at One of the Tenets

- **What does “All resource authentication and authorization are dynamic and strictly enforced before access is allowed.” mean in a z/OS environment?**
  - The authorization/access control mechanisms cannot be bypassed; The operating system must have integrity
  - Access control is based on a trusted identity
    - Multifactor Authentication is essential to ensuring a trusted identity

What Can I do Now?

- **The “Zero Trust Basics” section (p.1) that the goal of Zero Trust is:**
  - “…to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible**”**

What Can I do Now?...

- **What can I look for right *now?***
  - *Anything which can be leveraged to undermine the access control mechanisms*
  - *Any security definition which allows non-granular access*
  - *Any system privilege which allows non-granular access*

What Can I do Now?...

Top Ten Critical Assessment Findings in Mainframe Environments:

1. User IDs with no password interval
2. Inappropriate use of z/OS UNIX UID(0)
3. Improper/lack of UNIXPRIV controls
4. Started task user IDs not PROTECTED
5. Excessive access to z/OS UNIX file system data sets
6. Excessive Access to APF libraries
7. Excessive Access to SMF data sets
8. Production data sets that anyone can access (UACC > NONE, GAC, ID(*))
9. Unauthorized started tasks defined as TRUSTED or PRIVILEGED
10. Critical data sets that anyone can UPDATE (or READ in some cases)

Source: Vanguard Integrity Professionals

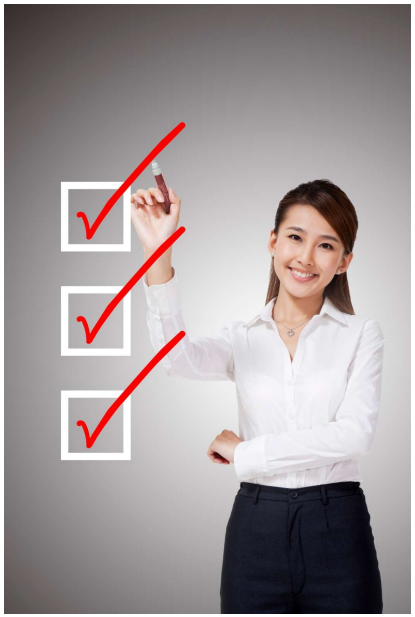
What Can I do Now with What I Have Now?

- **z/OS and RACF have many tools that extract and evaluate information about the current environment which can be directly used :**

  - IBM Health Checks for z/OS
  - The RACF Search Command
  - The RACF Database Unload Utility
  - The RACF Data Security Monitor
  - *… and others*

RACF Health Checks

RACF provides 27 health checks in the IBM Health Checker for z/OS that examine:



- **The protection of key system data sets and resources:**
  - RACF_SENSITIVE_RESOURCES
  - RACF_RRSF_RESOURCES
- **The active status of these key general resource classes:**
  - TEMPDSN, TAPEVOL, TSOAUTH, JESSPOOL, OPERCMDS, CSFSERV, CSFKEYS, JESJOBS, FACILITY
- **The status of the one pre-defined RACF user ID**
  - RACF_IBMUSER_REVOKED

RACF Health Checks…

- **RACF system options:**
  - RACF_AUDIT_CONTROLS
  - RACF_BATCHALLRACF
  - RACF_ENCRYPTION_ALGORITHM
  - RACF_ERASE_ON_SCRATCH
  - RACF_PASSWORD_CONTROLS
  - RACF_PROTECTALL_FAIL

- **RACF operational configuration:**
  - RACF_ADDRESS_SPACE
  - RACF_SYSPLEX_COMMUNICATION
  - RACF_GRS_RNL
  - RACF_ICHAUTAB_NONLPA

RACF Health Checks…

- **Other RACF Checks**
  - RACF_CERTIFICATE_EXPIRATION
  - RACF_PTKTDATA_CLASS
  - RACF_UNIX_ID
  - Installation-defined checks (No code… just profiles!)

But Wait, there's More!

- **It's Not Just RACF!**
  - JES_NJE_SECURITY
  - CSV_APF_EXISTS
  - CSAPP_FPTD_ANONYMOUS_JES
  - CSAPP_MVRSHD_RHOSTS_DATA
  - CSAPP_SMTPD_MAIL_RELAY
  - CSAPP_SNMPAGENT_PUBLIC_COMMUNITY
  - … and more

RACF_SENSITIVE_RESOURCES Health Check

- **The RACF_SENSITIVE_RESOURCES Health Check examines the profiles protecting key system data sets to validate that excessive access is not granted to all users**

- **The check examines the universal access (UACC), ID(*) access list entry and the WARNING profile attributes of these data sets:**
  - The protection of key system data sets:
    - Authorized program facility (APF)
    - RACF data base
    - PARMLIB
    - Link List
    - System REXX
    - ICSF

- **You can specify a user ID whose authority will be checked**

- **The RACF_RRSF_RESOURCES check does the same for the RRSF INMSG and OUTMSG data sets**

RACF_SENSITIVE_RESOURCES Health Check…

- **The RACF_SENSITIVE_RESOURCES also examines key general resource profiles which are used to grant users significant system privileges, such as the ability to:**

  - Become a z/OS UNIX System Services superuser
  - Change file attributes on a z/OS UNIX file (APF authorized, owner…)
  - Perform password resets
  - Issue certain sensitive z/OS operator commands (such as SET PROG, HALT, SLIP)
  - The ability to issue certain TSO commands (ACCT, CONSOLE, OPER, TESTAUTH, PARMLIB)

The Health Checker for z/OS Bottom Line

Net: All Health Checker for z/OS exceptions must be investigated and either:

- Addressed by the appropriate configuration change
- Determined to be not applicable and the health check altered to no longer raise an exception

The RACF SEARCH Command

The RACF SEARCH command returns the list of profiles in a class to which the user has either administrator authority or READ authority

Performing a SEARCH command from a user ID which has no administrative authorities will reveal those profiles to which the user has READ authority.

- A LISTDSD (for data sets) or RLIST (for general resources) command can be used to see how the user was granted access and what access the user has

- Access granted by UACC, ID(*) access list entry, or GLOBAL profile represents a violation of the Zero Trust access granularity principle.

The RACF SEARCH Command…

Interesting classes:

- DATASET (with the NOMASK option)
  - Especially with the list of APF data sets which can be read by unauthorized programs
- FACILITY
- UNIXPRIV
- SURROGAT
- USER with the UID(0)

The RACF Database Unload Utility

One essential utility in your tool belt is the RACF Database Unloa Utility (IRRDBU00), which:

- Unloads a RACF data set into a sequential file that can be eas viewed, loaded into a relational data base or processed with report-generation tools (such as the DFSORT ICETOOL utility)

- All profiles in the RACF data base are unloaded and all fields decoded except these fields which are ignored:
  - Encrypted fields
  - Fields marked as “reserved for IBM”

- Requires READ authority to the input RACF data set
  - Hmmm…. Could we do better from a Zero Trust viewpoint? Yes! `PERMIT … WHEN(PROGRAM(IRRDBU00))`

The RACF Database Unload Utility…

RACF ships 30+ DFSORT ICETOOL reports in 'SYS1.SAMPLIB(IRRICE)', several of which are directly applicable to your Zero Trust journey:

Name	Description
ALDS	IDs with ALTER Authority to Discrete Data Set Profiles
IDSC	Data Set Conditional ACLs with ID(*) Other Than None
IDSS	Data Set Standard ACLs with ID(*) Other Than None
IGRC	General Resource Conditional ACLs with ID(*) Other Than None
IGRS	General Resource Standard ACLs with ID(*) Other Than None
SUPU	z/OS UNIX System Services Super Users (UID of 0)
UADS	Data Set Profiles with a UACC Other Than None
UAGR	General Resource Profiles with a UACC Other Than None
UGLB	Users with Extraordinary Authorities
UGRP	Users with Extraordinary Group Authorities
WNDS	Data Set Profiles in WARNING Mode
WNGR	General Resource Profiles in WARNING Mode

RACF Data Security Monitor (DSMON)…

DSMON is a program that reports on the status of the security environment at your installation, in particular, on the status of resources that RACF controls.

While all of its reports are of interest from a Zero Trust perspective, these are of special interest:

- **Program Properties Report**
  - What programs are there and why?
- **RACF Exits Report**
  - What exits are in place, why are they there, and what do they do?
- **Selected User Attribute Report**
  - What users have global authorities like SPECIAL, OPERATIONS ”

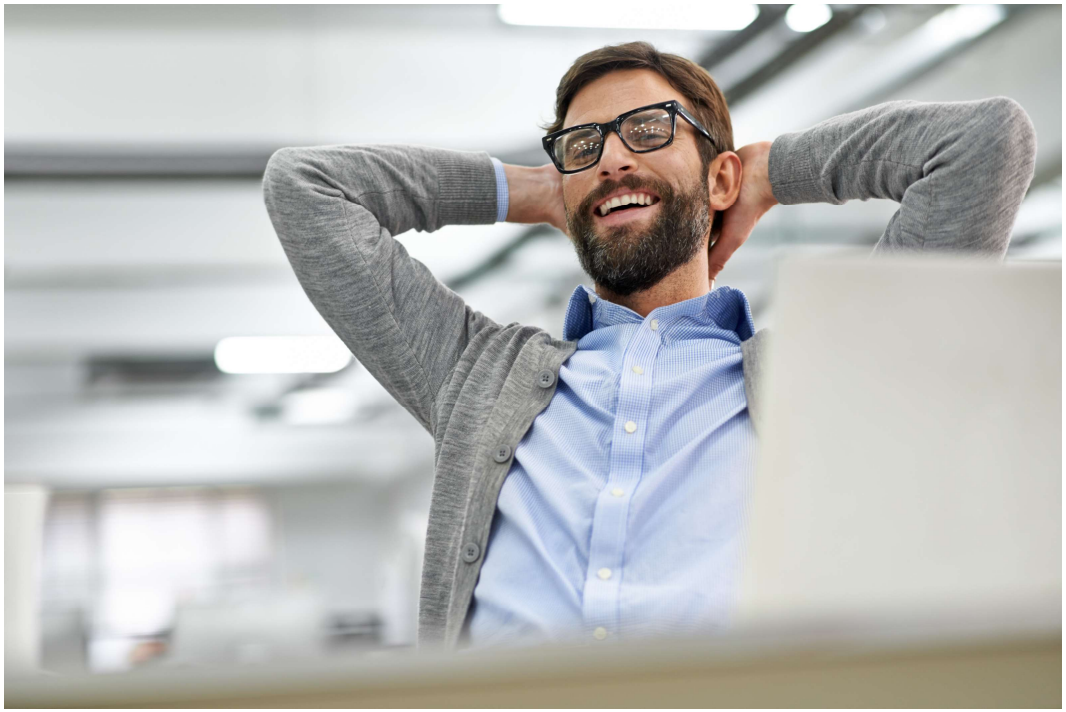
RACF Data Security Monitor (DSMON)

More interesting DSMON reports:

- **Started Procedures Report**
  - What started procedures run TRUSTED? PRIVILEGED?
- **RACF Class Descriptor Table Report**
  - What classes are active?
- **RACF Global Access Table Report**
  - What classes have global access profiles defined?

That’s it?

You might think that we are done now…



That’s it?

But, you would be wrong.

We are Merely Scratching the Surface!

We've focused on what you can do now, which is an essential start to your Zero Trust, but we are barely "scratching the surface" on your Zero Trust Journey.

Other essential steps on the Zero Trust Journey:

- Multifactor authentication, not just for a subset of users
- Establishment of a comprehensive logging policy and the automated review of those log records
- Establishment of a configuration management policy with automated compliance evaluation


DID YOU KNOW?
QUIZ TIME!
TRIVIA NIGHT

Questions

- **Question 1: The RACF Health Check which examines key system data sets and general resources for a minimal set of protections is:**
  - RACF_PROTECTING_CORRECTLY
  - RACF_SENSITIVE_RESOURCES
  - RACF_OSRS_PROTECTED
  - RACF_MAKE_ME_SECURE

Questions

- **Question 2: The RACF_SENSITIVE_RESOURCES check reviews:**
  - Use profiles to ensure that only non-human users have UID(0) assigned
  - The encryption status of your RACF Remote Sharing Facility (RRSF) data sets
  - Key operating system data objects and resources for excessing access
  - RACF SETROPTS options, such as password encryption algorithm and password rules

Questions

- **Question 3: An example of a data set which is not checked by the RACF_SENSITIVE_RESOURCES check is:**
  - APF
  - Link List
  - RACF data base
  - TCP/IP configuration data

Questions

- **Question 4: The RACF_SENSITIVE_RESOURCES and RACF_RRSF_RESOURCES checks examine the profile items below except:**
  - UACC
  - ID(*)
  - WARNING attribute
  - ERASE attribute

Questions

- **Question 5: The journey to Zero Trust is addressing these generally accepted security principles:**
  - Least Privilege
  - Defense in Depth
  - Fail Securely
  - All of the above

Questions

- **Question 6: Which of the following is true?**
  - Creating a Zero Trust environment is a simple matter of ensuring that all data is protected by RACF profiles or SETROPTS options
  - Zero Trust is an architecture that is defined in NIST Special Publication 800-207
  - Transitioning to Zero Trust is a journey and cannot simply be accomplished with a wholesale replacement of technology
  - All that you need to do to implement Zero Trust is to attend Vanguard conferences

Parting Thoughts

- Zero Trust is a journey with a destination that can be imagined, but which can never be reached. ***The journey is the destination.***

Zero Trust and RACF®

Moving Towards Least Access Privilege

Mark Nelson, CISSP®, CSSLP®
IBM® Poughkeepsie

November 2024