DEEP SEC | VIENNA | 2010

Jennifer Jabbusch, CISSP, HP MASE, JNCIA-AC
Infrastructure Security Specialist
Carolina Advanced Digital, Inc. http://cadinc.com
Blog and news http://SecurityUncorked.com

Identicate & AUTHENTify

Improving future implementations
to address real security challenges

Identicate &AUTHENTify

I. INTRO

Introduction

Identification and authentication are two fundamental concepts of security frequently confused and obscured. Without a proper grounding, addressing current and future challenges becomes more cumbersome and costly. This talk lays the foundation for effective identification and authentication, outlining current practical applications and guiding a thought-provoking theoretical discussion of future considerations for these essential concepts. Participate in the discussion that will drive the future of identification, trust models, national IDs and the use (or misuse) of biometrics and other identifying attributes.

Identicate &AUTHENTify

II. BACKGROUND

Background

About me, our company and how I arrived here...

Jennifer Jabbusch is an infrastructure security specialist and consultant with Carolina Advanced Digital, Inc. Jennifer has more than 15 years experience working in various areas of the technology industry. Most recently, Ms. Jabbusch has focused in specialized areas of infrastructure security, including Network Access Control, 802.1X and Wireless Security technologies. Jennifer has consulted for a variety of government agencies, educational institutions and Fortune 100 and 500 corporations. In addition to her regular duties, she participates in a variety of courseware and exam writings and reviews, including acting as subject matter expert on Access Control, Business Continuity and Telecommunications, and lead subject matter expert in the Cryptography domains of the official (ISC)2 CISSP courseware (v9). You can find more security topics and musings on her security blog at http://SecurityUncorked.com

Identicate &AUTHENTify

III. WE'RE DOING IT ALL WRONG

Why we're doing it all wrong

My problem with identification and authentication in IT and how these simple conversations led me down a path to discover more on identity.

Why we're doing it all wrong

How I came to realize…

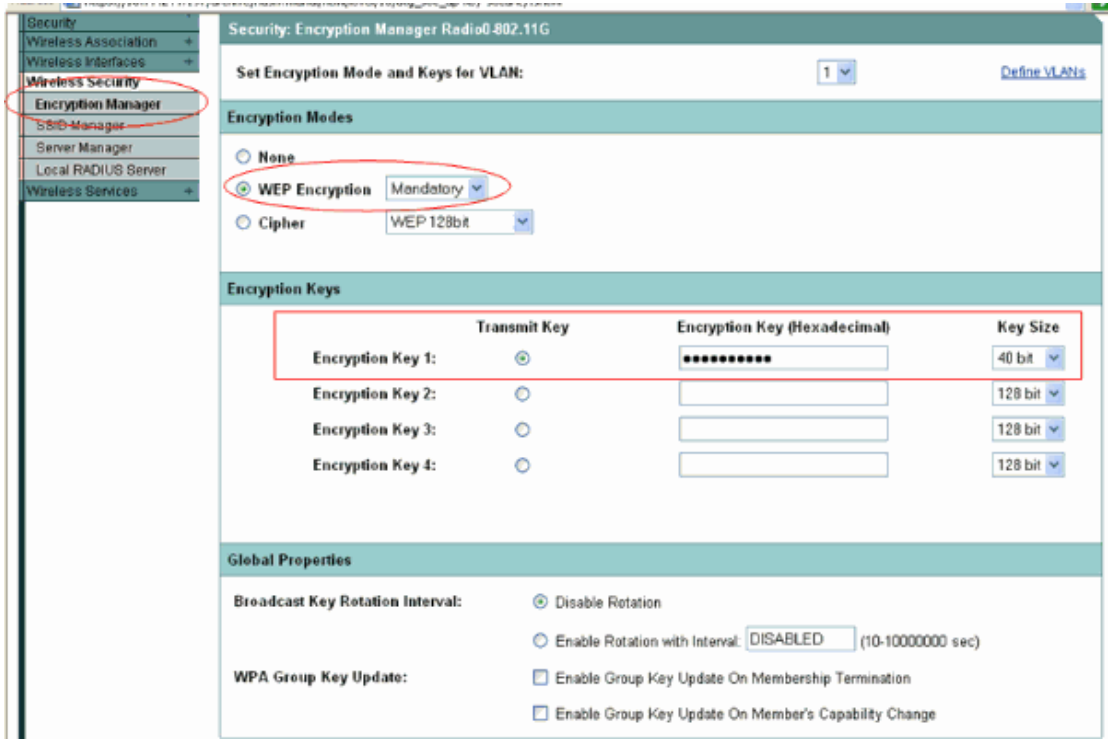
WE'RE DOING IT ALL WRONG!

Why we're doing it all wrong

I have two problems with this scenario…

Example 1

Wireless PSK



Problem: We're neither identifying or authenticating

Why we're doing it all wrong

Example 2

Network device MAC-authentication

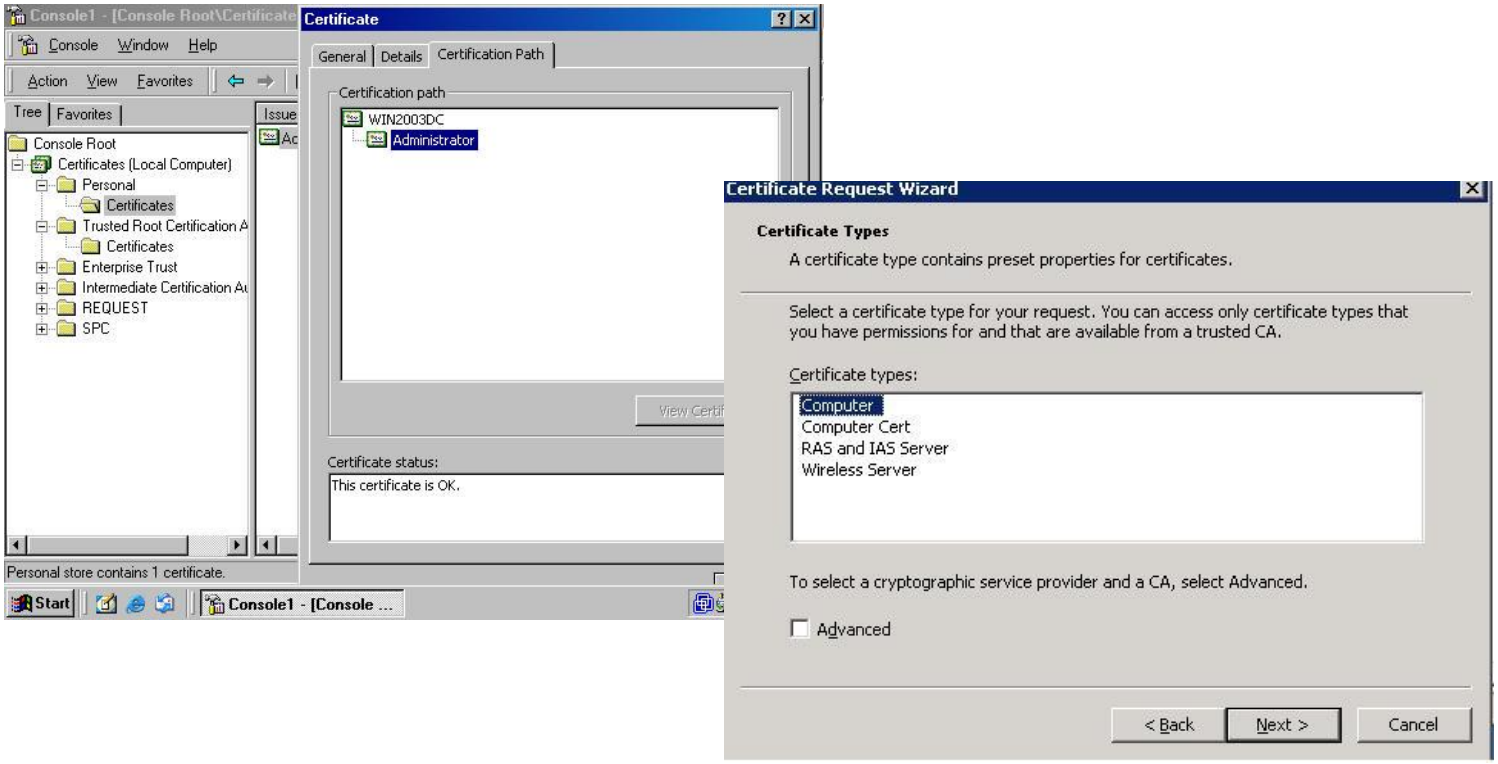
```
5412zl(config)# aaa port-access mac-based a5

LACP has been disabled on 'port-access' enabled port(s

5412zl(config)# aaa port-access mac-based a5 auth-vid
5412zl(config)# aaa port-access mac-based a5 unauth-vi
5412zl(config)# exit
5412zl#
```

Problem: We're identifying but not authenticating

Why we're doing it all wrong

Example 3

Certificates for credentials



Problem: We're authenticating the machine but not the user

Why we're doing it all wrong

How do we fix it? We have to start by defining the underlying concepts and terminology of identity and authentication. What do these things mean, when do we need each and how do we go about implementing them.

Identicate &AUTHENTify

IV. DEFINING CONCEPTS

Defining Concepts

Identity

"Identity is a relation between our cognitions of a thing, not between things themselves."

-Sir W. Hamilton

The term cognition (Latin: cognoscere, "to know", "to conceptualize" or "to recognize") refers to a faculty for the processing of information, applying knowledge, and changing preferences. Cognition, or cognitive processes, can be natural or artificial, conscious or unconscious

- in philosophy, identity is whatever makes an entity definable and recognizable, in terms of possessing a set of qualities or characteristics that distinguish it from other entities. Or, in layman's terms, identity is whatever makes something the same or different.
- the state of having unique identifying characteristics held by no other person or thing (I disagree with this one since identification in the real world may not be unique)
- the distinguishing character or personality of an individual
- the set of behavioral or personal characteristics by which an individual is recognizable as a member of a group

Defining Concepts

In several studies from both the US and European organizations on identity management, there are several proposed models of identity that are interesting.

Of particular note is the notion of a model separating identity into two overarching functions:

1) Identity as a representation
2) Identity for identification

Defining Concepts

Identification

Question: Must an ID be unique?
There's a difference in how we perceive that in digital versus real world. In the IT world, each ID must be unique. In the real world, each ID may be unique within a certain context or even logical or geographic area

- The function of identification is to map a known quantity to an unknown entity so as to make it known. The known quantity is called the identifier (or ID) and the unknown entity is what needs identification. A basic requirement for identification is that the ID be unique. IDs may be scoped, that is, they are unique only within a particular scope. IDs may also be built out of a collection of quantities such that they are unique on the collective.
- Identification is the capability to find, retrieve, report, change, or delete specific data without ambiguity. This applies especially to information stored in databases. In database normalization, it is the central, defining function to the discipline.

Defining Concepts

Identify

- to prove or recognize as being a certain person or thing; determine the identity of
- to recognize or establish as being a particular person or thing; verify the identity of
- Biology . to determine to what group (a given specimen) belongs.
- Psychology . to associate (one or oneself) with another person or a group of persons by identification.

A thought: I disagree with portions of these statements in practice; identification does not necessarily encompass 'proving' identity or 'verifying' the identity of.

Defining Concepts

Authenticate

1.the ownership factors: Something the user has (wrist band, ID card, security token, software token, phone, or cell phone)
2.the knowledge factors: Something the user knows (a password, pass phrase, or personal identification number (PIN), challenge response)
3.the inherence factors: Something the user is or does, fingerprint, retinal pattern, DNA sequence, signature, face, voice, unique bio-electric signals, or other biometric identifier

- Authentication (from Greek, real or genuine, from authentes; author) is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the subject are true
- "authentification" is a French language variant of this word
- The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something you know, something you have, or something you are

Identicate &AUTHENTify

Defining Concepts	.	.
Identity	**Identification**	**Authentication**
The set of characteristics by which a thing is recognizable	Method by which we determine and recognize the thing	Validation that the thing is who or what he/she/it claims to be

Thing = a person, device, user

Identicate &AUTHENTify

V. IDENTIFYING FACTORS OR TRAITS

Identifying factors or traits

What things, traits, factors or characteristics can we use to identify and/or authenticate people or things?

- Name
- Unique number (serial number, SSN, barcode)
- Knowledge of something (password/PIN)
- Physical possession of something (keys/certificates)
- Physical traits or behavior (biometrics or measurable attributes, size, weight)

- Location or location history
- Age
- Relationship or affiliation
- Accreditation or certification
- Gender
- Race
- Behavioral patterns
- Species (plants, animals)
- DNA, blood
- Financial attributes
- … others?

Identifying factors or traits

Now, let's see how these concepts fit in to the technical and real world domains.

The first steps in fixing the problem were to recognize it and articulate the definitions of the components. Next we have to understand what the drivers are in each implementation scenario so we can clearly outline our goals and create a plan to get from A to B.

Identicate &AUTHENTify

VI. IDENTITY & AUTHENTICATION IN THE TECHNICAL DOMAIN

Identity & Authentication in the Technical Domain

What are drivers for identity and authentication in technical domain?

- Securing access to resources
- Logging for change management
- Meeting regulatory compliance
- Action audits and accountability
- Maintaining integrity and availability of systems

Identity & Authentication in the Technical Domain

When do we use identity and authentication in the technical domain?

- Wireless network access
- User domain logon
- Remote access
- Managing network devices and users
- Device or machine authentication to network or domain
- Physical access to data centers
- Correlating actions to users
- Accessing stored data, voicemail, email
- Account management validation (vendors)
- Aggregation and correlation of event data, SIEM, Metadata (IF-MAP)

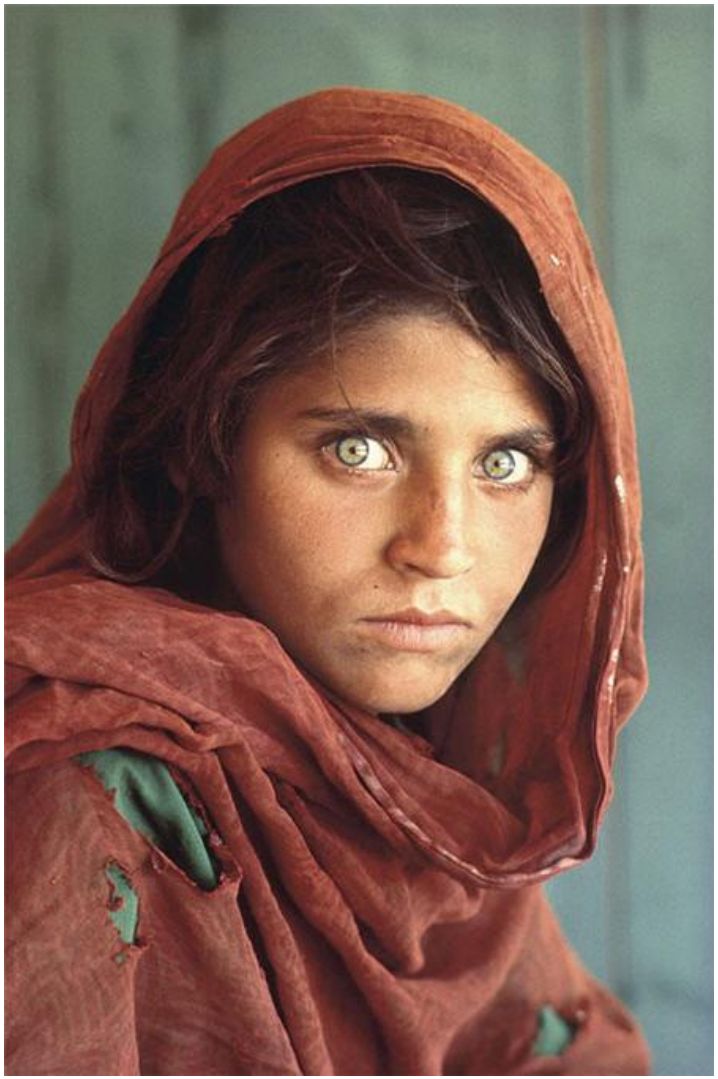
Identity & Authentication in the Technical Domain

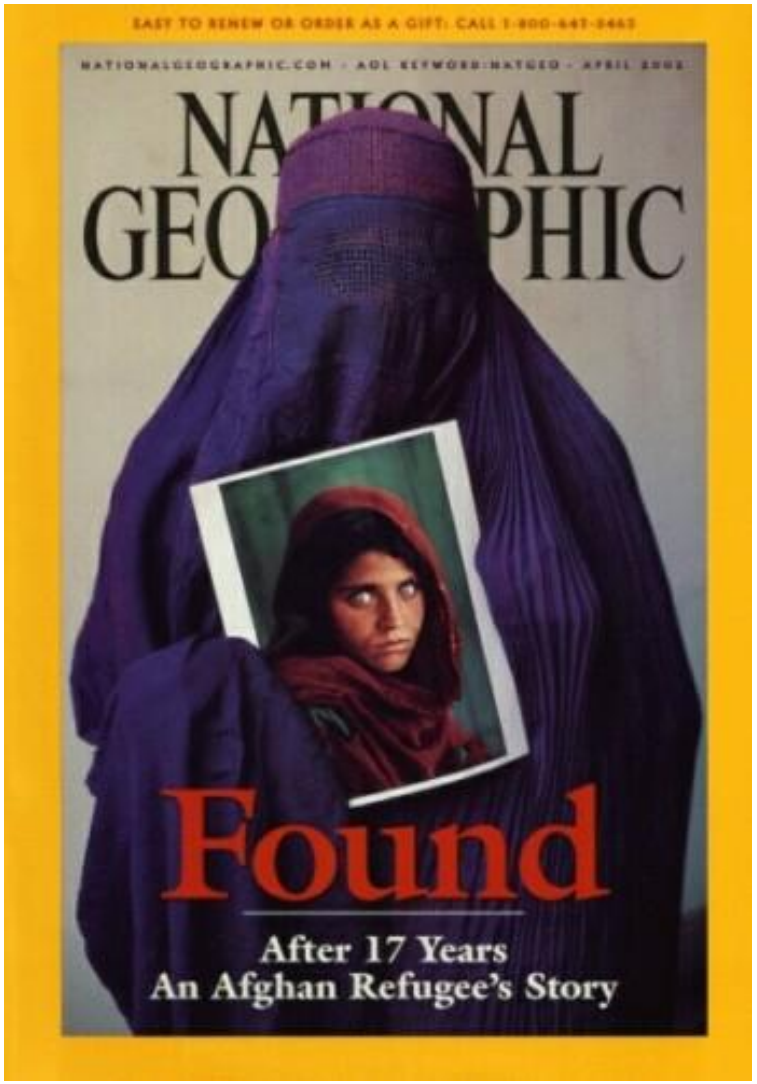
What do we use for identity and authentication here?

- Static user credentials (passwords)
- Dynamic user credentials (OTP, texted passwords)
- Logical keys (certificates or crypto keys)
- Device credentials (machine ID)
- RFID cards
- MAC addresses on hardware
- Source IP addresses at gateways
- Behavioral analysis (NBAD)
- Security event correlation (SIEM, TNC IF-MAP)
- Biometrics (ID or validate ID)

What's right or wrong with each of these?

Identity & Authentication in the Technical Domain





Identity & Authentication in the Technical Domain

Now, let's see how these same concepts fit in to the real world.

Identicate &AUTHENTify

VII. IDENTITY & AUTHENTICATION IN THE WORLD DOMAIN

What are drivers for identity and authentication in real world?

- Securing access to accounts
- Collecting historical data for trending
- Using historical data to minimize risk
- Validating attributes such as age and gender
- Matching people to credentials or authorizations
- Protecting financial resources
- Managing legal disputes
- Monitoring travel and movement
- Validate uniqueness of data (prevent duplicates in surveys/votes)

Identity & Authentication in the World Domain

When do we use identity and authentication in the real world?

- Online purchases, payments and banking
- Establishing and managing credit (credit cards, utilities, loans)
- Establishing or claiming insurance (house, car, health)
- Medical situations (healthcare, prescriptions)
- Driving (drivers license and endorsements)
- Traveling (passports, VISAs)
- Voting
- Attending school
- New employment
- Tracking pets
- Tracking merchandise

Identity & Authentication in the World Domain

What do we use for identity and authentication here?

- Identification cards or
- Certified documents
- Licenses
- Key fobs or dynamic code cards
- RFID
- Biometrics
- Loyalty or membership cards
- Collections of data

What's right or wrong with each of these?

Identity & Authentication in the World Domain

How do these play in to privacy issues?

Identity and privacy in the real world

What's your limit for sharing info?

Microdata and identity

How do you feel about microdata collected (web browsing habits, frequent searches, shopping habits in stores or online)

Content of data versus use of data

The type of data they collect versus the use of that data after it's collected. Is information collected and truly aggregated anonymously for statistics less intrusive than data collected to profile your habits and target marketing?

Consensual sharing

Which of these might you provide if they weren't linked to ANY other data sets (ie your name, address or employer).

- Household income
- Postal code
- Relationship status (married, single, divorced)
- Household (number of kids, pets)
- Sex (male/female)
- Age group (21-30, 31-45, etc)
- Household (number of vehicles)
- Birth date (month/day only)
- Interests
- Occupation

Consensual sharing

Which of these might you provide if they weren't linked to ANY other data sets (ie your name, address or employer).

- Household
- Postal c
- Relation
- Household
- Sex (ma
- Age grou
- Household (number of vehicles)
- Birth date (month/day only)
- Interests
- Occupation

A data set of just a
-birth date
-zip code and
-gender
are enough to unique identify
87% of Americans.

Identity & Authentication in the World Domain

What concepts apply (or should apply) globally to both technical and real world domains?

Identicate &AUTHENTify

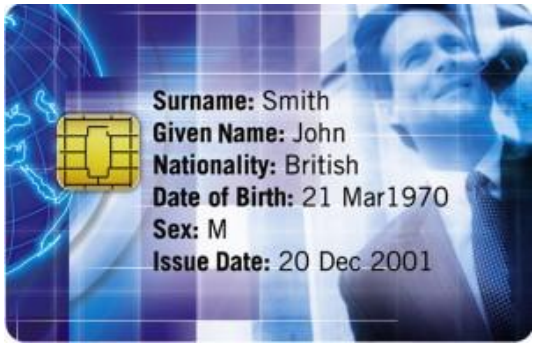
VIII. GLOBAL CONCEPTS OF IDENTITY & AUTHENTICATION

Concepts of Identity and Authentication globally (all domains)

Exploring similarities and differences in concepts of identity and authentication in both the technical and world domains.

The following content may present more questions than answers.

How many IDs and what kind should we have?



How many IDs and what kind should we have?

- Distributed and federated IDs
- National IDs in the world
- Bundle of sticks concept
- IT versus World: Multiple MAC addresses versus multiple personal identities
- IT versus World: Aggregation of meta-data in TNC IF-MAP versus national repositories of data and movement of a person

Specific versus ambiguous identity

- Specificity of an identity: do we need to identify a specific person/thing or simply verify a requirement (ie age or certification) is met?
- When do we need each?

Changing and Moving Rights

- Addressing identity theft and changes in rights
- Revocation
  - Revocation and identity
  - Revocation and authentication
    - Revocation of things you have
    - Revocation of things you know
    - Revocation of things you are/do
- Revocation, changes and biometrics
  - Biometrics in Identity
  - Biometrics in Authentication or Verification
  - Changing inherent biometric properties

Identicate &AUTHENTify

IX. CLOSING THOUGHTS

Closing thoughts and calls to action

1. While you knew that identity and authentication were different, hopefully now I've given you a clear set of parameters to define and apply each concept, based on your needs.
2. Micro and macro: How we address identity and authentication in one domain (technical, real) will affect the other(s). Once a model is founded that works and is modular, scalable and flexible, it will applied to other aspects of identity management.
3. As you move forward be aware of these differences and impacts of one system on another. Use identification and authentication where appropriate in EVERY system or process and document the needs and implementation of each step.
4. Remember identity is hard to define and even harder to demonstrate. Think about what it means to you and how something should be identified. What traits make up this 'thing' and what do you need to know about it for your purposes?
5. Biometrics are not the end-all be-all for identification of people. They're spoofable, they're flawed, they may be intrusive, they can change when we want them to stay the same and they may stay the same when we wish we could change them.
6. Think about identity as a bigger picture, consider the pros and cons of federated and distributed identity models in the real world and participate in discussions of identity, authentication, trust and privacy whenever possible.
7. WE are shaping the future of identity right now and what we (as a group) deem to be acceptable will in turn manifest as technology to be "in general public use". Once a technology or process hits this stage, we have little or no rights as members of a community to protect ourselves against it.

Thank you.

DEEP SEC | VIENNA | 2010

Jennifer Jabbusch, CISSP, HP MASE, JNCIA-AC
Infrastructure Security Specialist
Carolina Advanced Digital, Inc. http://cadinc.com
Blog and news http://SecurityUncorked.com

Identicate &AUTHENTify

Improving future implementations
to address real security challenges