Authentication Issues for Financial Services

And some related issues

Interisle
Consulting Group

Chuck Wade
16-May-2005
508 625-1137
Chuck@Interisle.net

Agenda

Interisle Consulting Group

- A model for placing authentication in context
- Examples of modern authentication problems
  - "Identity Theft"
  - Role of Biometrics
  - The Non-Repudiation Myth
  - Consumer/Merchant Authentication
- Some real-world requirements
- The new players
- Who wins? Who loses?

What is authentication?

Interisle Consulting Group

- Authenticate: Determine to some level of assurance that a party is entitled to a specific set of credentials—*i.e.*, a procedure or mechanism that tests entitlement claim
- Credential: That which gives a title or claim to credit or confidence [*syn.* certificate]
  - Name of individual or organization, address, telephone #
  - Bank account, credit card account (ability to pay)
  - Credit approval, letter of credit (statement of creditworthiness)
  - Social Security Number, driver's license number
  - Employee, badge number
  - Academic diploma, certificate of accreditation
  - Parent or guardian [of some child], Child of some parent

What authentication is not…

Interisle
Consulting Group

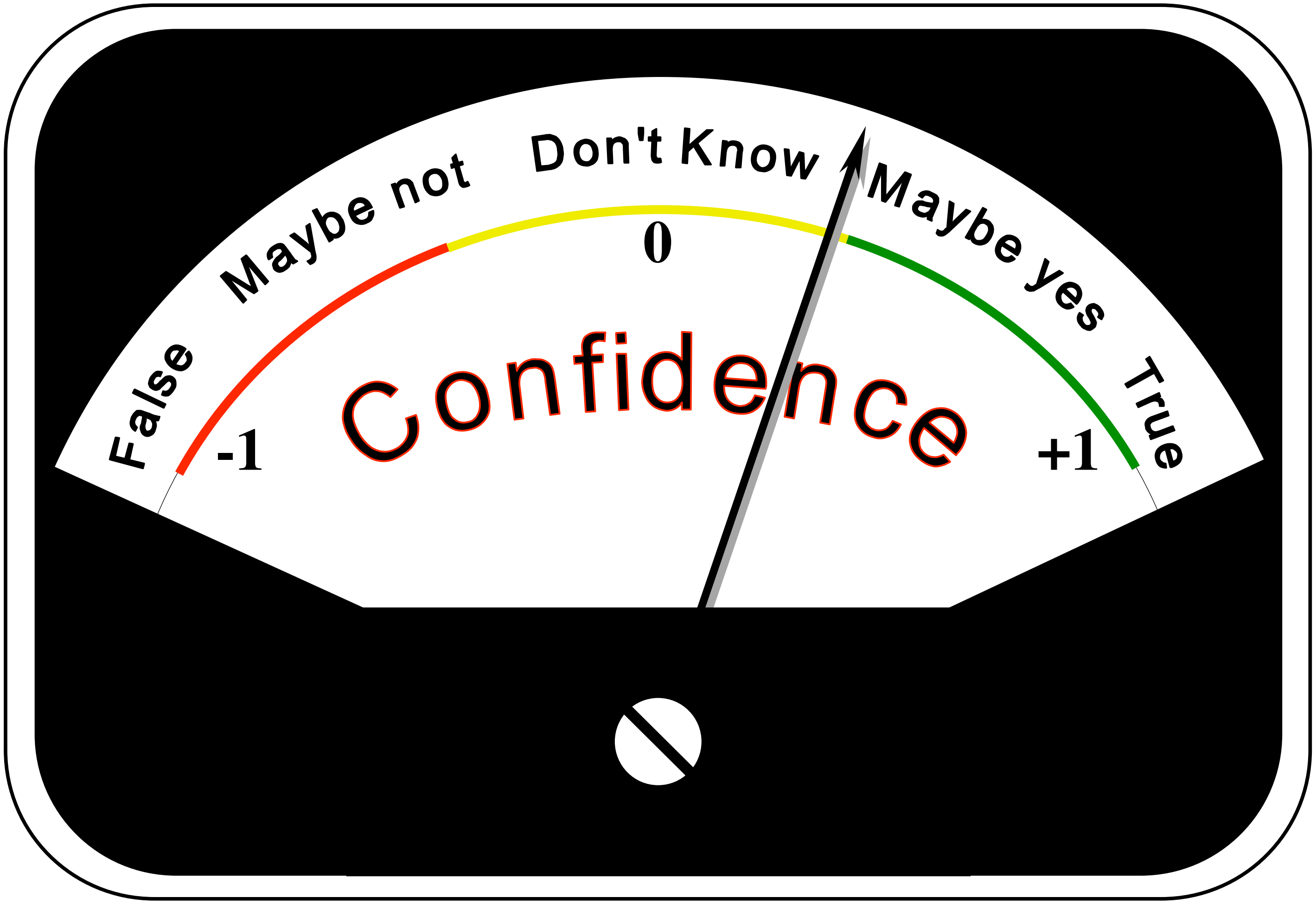
- Identification: distinguish some person or thing within a larger set by means of unique characteristics
  - No thesaurus lists authentication as a synonym of identification
- Authorization: an expression of intent or a commitment to abide by certain terms & conditions
- Access Control: determine whether or not a party should be granted access to information or resources
- Single Sign-On: consistent access control measures deployed across multiple systems in a convenient manner

Sources of confusion…

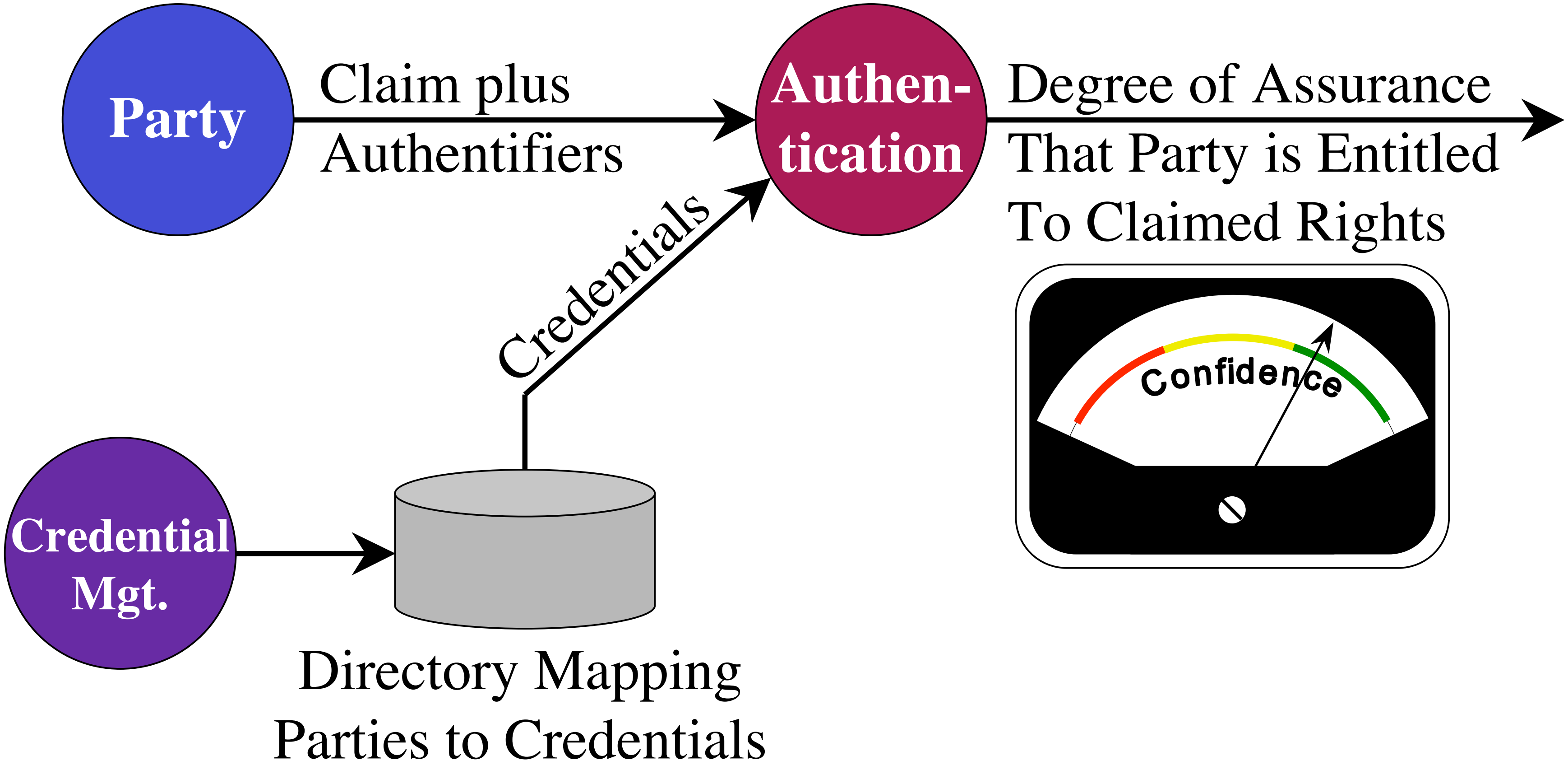
- Authorization, access control, & single sign-on can share common mechanisms & credentials with authentication
  - Authentication is one step in access control and single sign-on
  - Authentication is an elemental mechanism of authorization
- In the absence of strong authentication, identification has been used as a proxy
  - *A source of many modern problems!*
  - A whole industry has emerged to provide "identification" facts
- Authentication has been confused with enrollment or registration
  - Identity can be relevant during registration or enrollment for credentials

Authentication: Confidence Meter

Interisle Consulting Group



Authentication



Party

Claim plus Authentifiers

Authen-tication

Degree of Assurance That Party is Entitled To Claimed Rights

Credentials

Credential Mgt.

Directory Mapping Parties to Credentials

Registration

- The means by which one party formalizes a relationship with the registering party and is granted a set of credentials or is bound to credentials
  - Registration can be explicit or implicit
    - Explicit: Party specifically requests to register
    - Implicit: Party is registered as a byproduct of other actions (e.g., merchants often register customers upon completion of their first purchase)
  - The identity of the party receiving credentials may be relevant during registration (or may not be)
- Registration is generally based on some assessment of a party's fitness or "reputation"
- Third parties can act as registrars, and then vouch for credentials in subsequent authentications

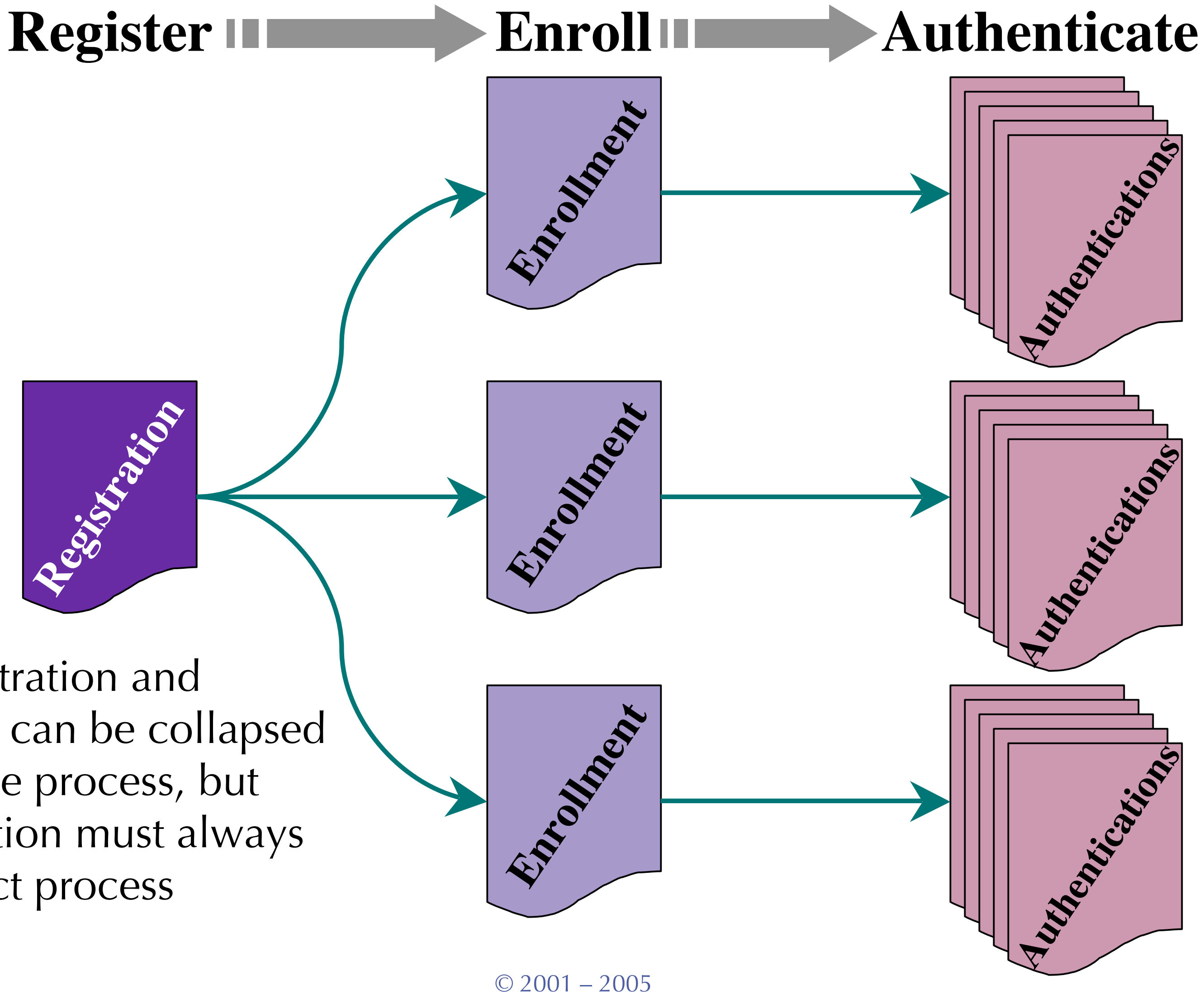
Enrollment

- While “enrollment” and “registration” are synonyms in normal English usage, it is helpful to draw the following distinctions:
    - Registration: a one-time process used to formalize a relationship between two or more parties
    - Enrollment: granting of rights or credentials based on an established relationship (prior registration)
        - Registration and enrollment may occur concurrently, and often do
        - There may be many enrollments (and de-enrollments) for any one registered relationship
        - E.g., A customer registers with a bank, and subsequently enrolls for a checking account, debit card, credit card, online access, CD, IRA, etc.

Authentifier binding

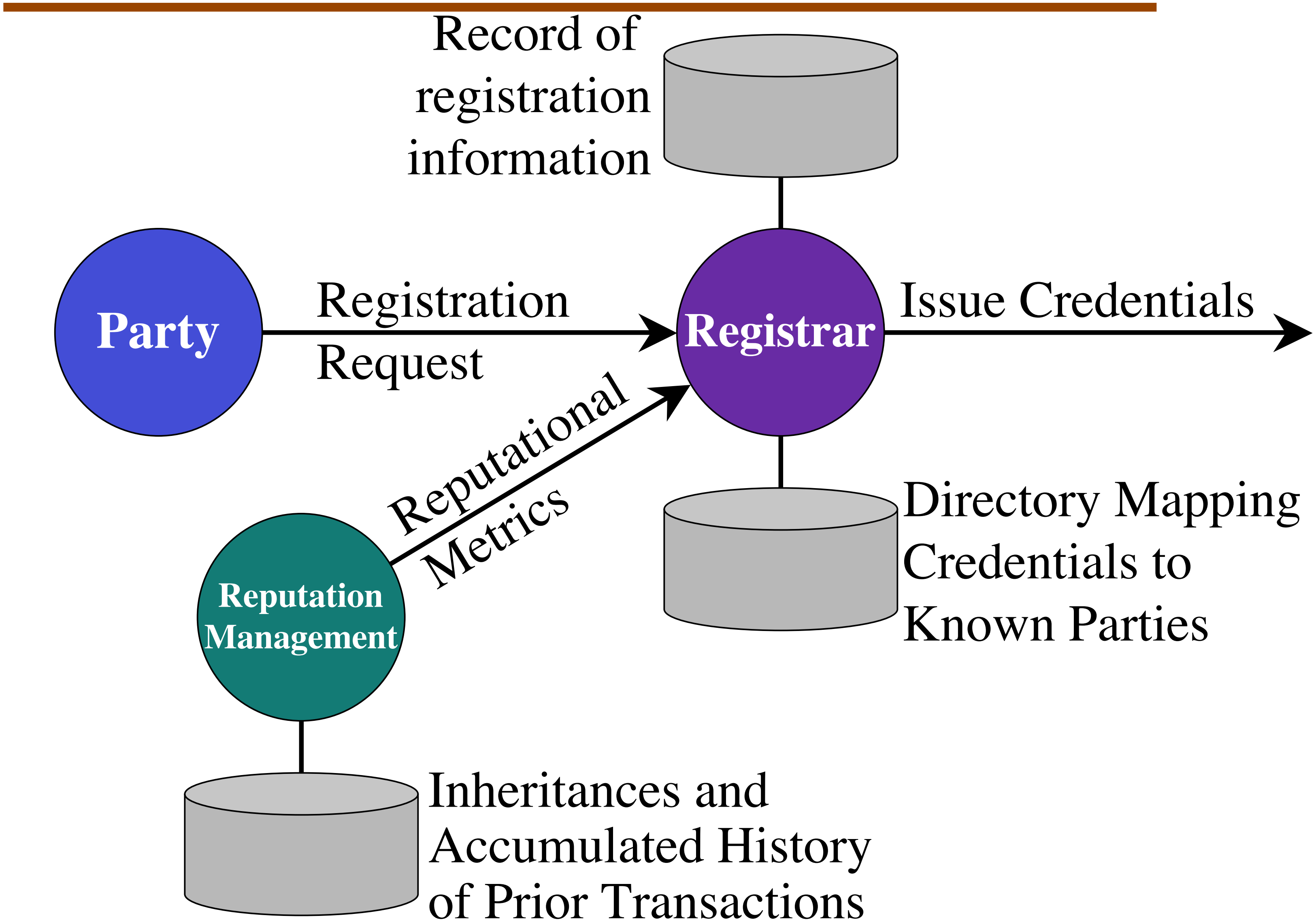
- Authentifier: any parameter or attribute that can be used to evaluate the authenticity of some claim or thing
  - "Authentication factor" is a commonly used synonymous term that is too often misused
  - Identifier is another near synonym
- An enrollment process is needed to bind an authentifier to an associated party
- Authentifier binding should be based on prior registrations and enrollments, but not directly coupled
  - Changing authentifier bindings should not disrupt existing relationships between parties

Cascading nature of Registration, Enrollment, Authentication



Note: registration and enrollment can be collapsed into a single process, but authentication must always be a distinct process

Registration



Record of registration information

Party

Registration Request

Registrar

Issue Credentials

Reputational Metrics

Reputation Management

Directory Mapping Credentials to Known Parties

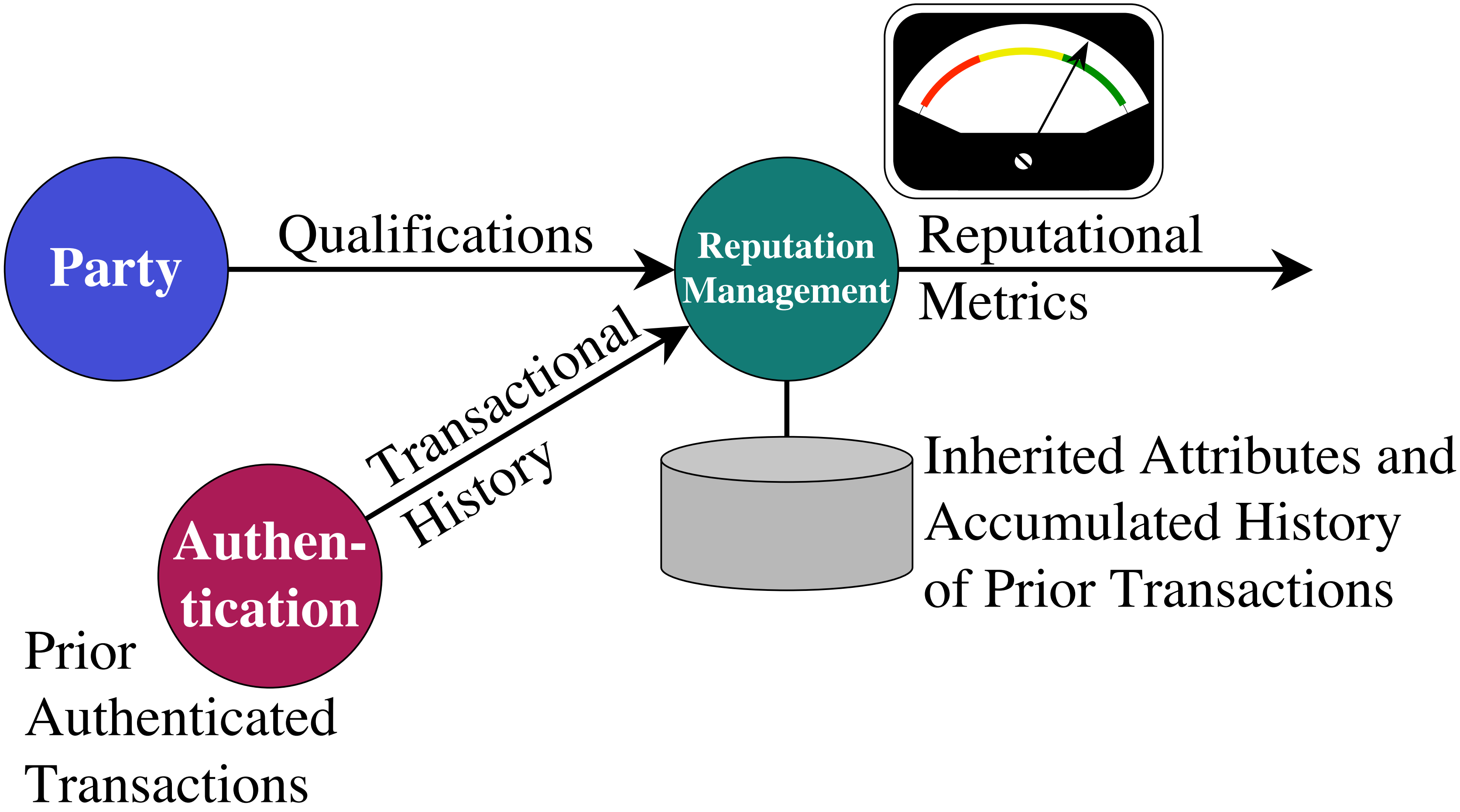
Inheritances and Accumulated History of Prior Transactions

Reputations

Interisle Consulting Group

- Reputation: a qualitative assessment of a party’s suitability for some role; often based on a history of prior transactions conducted by that party
  - Individual identity is founded on inheritance—a reputation of sorts (*e.g.*, pedigree)
  - Most reputations are cumulative:
    - Credit ratings
    - Professional or academic competence
    - Quality or integrity assessments
- Credentials are often used to state that a party meets certain criteria expressed as qualifications
- Many organizations involved in maintaining reputations
  - E.g., government agencies, law enforcement agencies, financial institutions, credit reporting agencies, insurance companies, bonding agencies, medical institutions, employers, merchants, professional organizations, academic institutions

Reputation

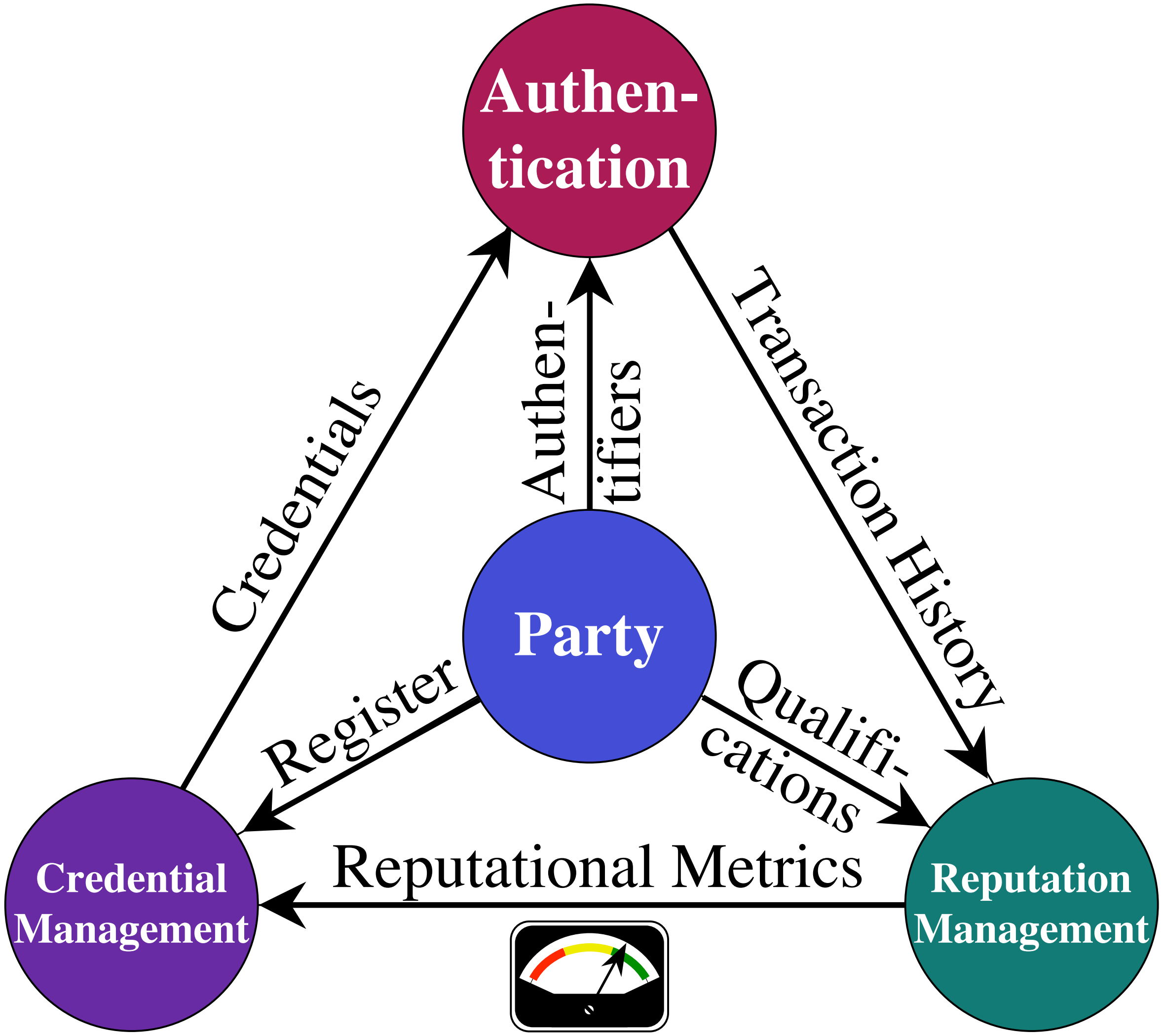

Party
Qualifications
Reputation Management
Reputational Metrics
Transactional History
Authen-tication
Prior Authenticated Transactions
Inherited Attributes and Accumulated History of Prior Transactions

Reputation Services

- Tracking and maintaining reputations is a well-established business in many industry segments
  - Credit reporting agencies are one widely-recognized example
  - The Internet has spawned an array of new reputation tracking services and enabled new extensions of traditional services
- Consumers also have access to reputation tracking services, in particular for financial institutions and merchants
- Reputation is taking on greater significance in the Internet age
- Many of the problems associated with authentication are really problems with management of reputations

The bigger picture…

Interisle
Consulting Group

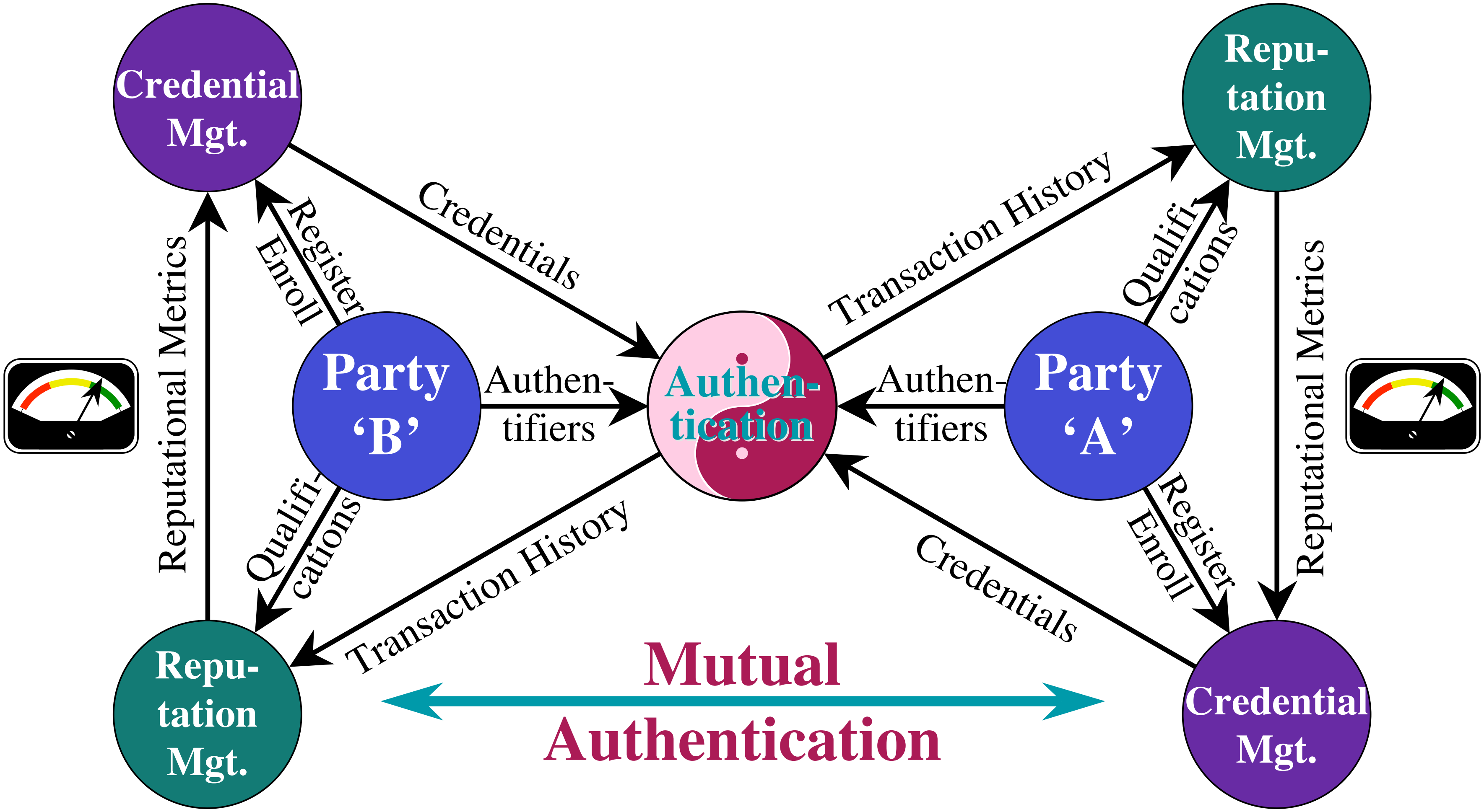


Mutual Authentication

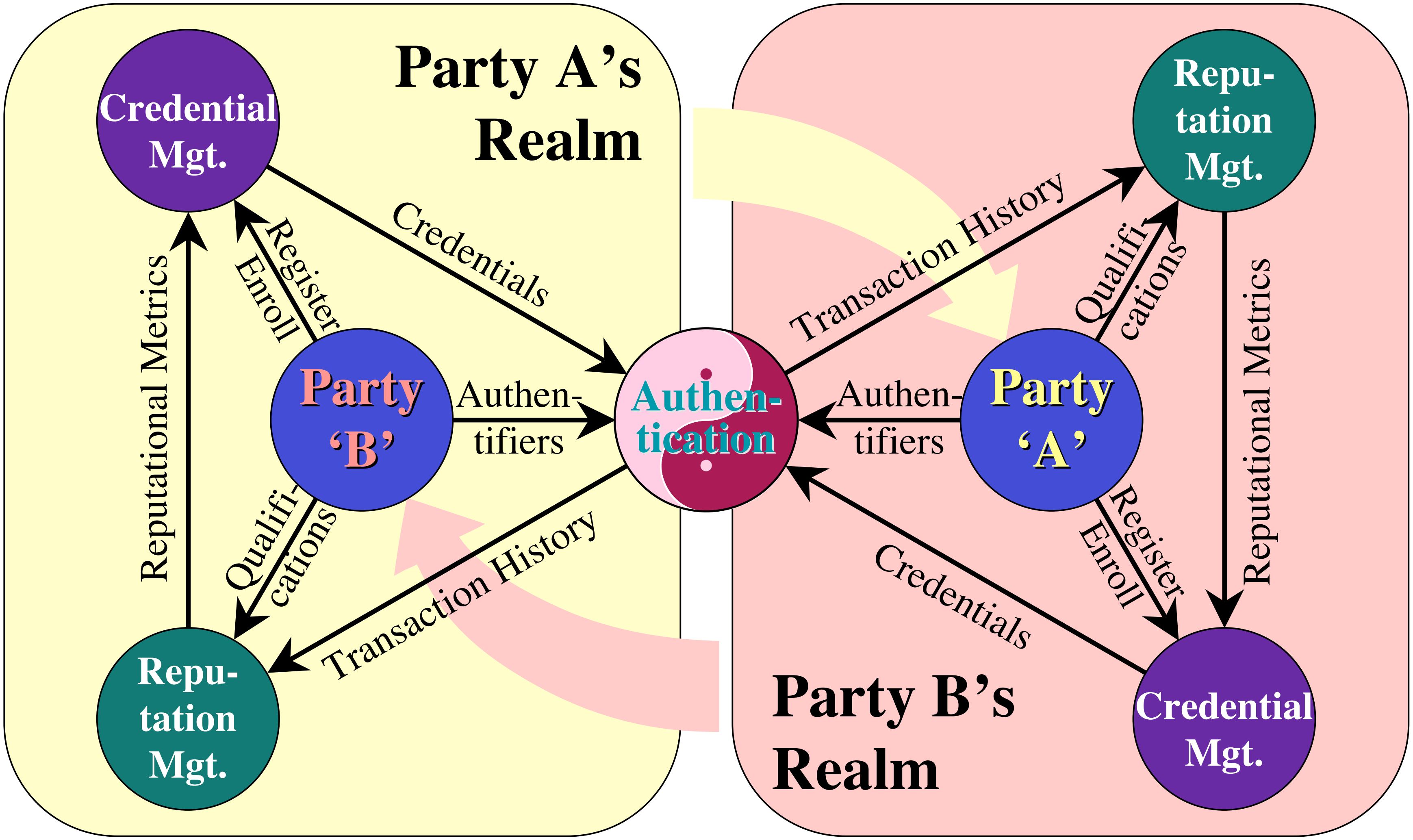
Interisle
Consulting Group

- The problem with authenticating only one party is that it takes two (or more) parties to communicate
- If only one party is authenticated then both parties are at risk
  - The authenticated party does not know if the other party is authentic
  - An imposter can impose themselves in place of the unauthenticated party
- Recent cyber exploits (e.g., phishing) have exploited weak one-way authentication

The still bigger picture…

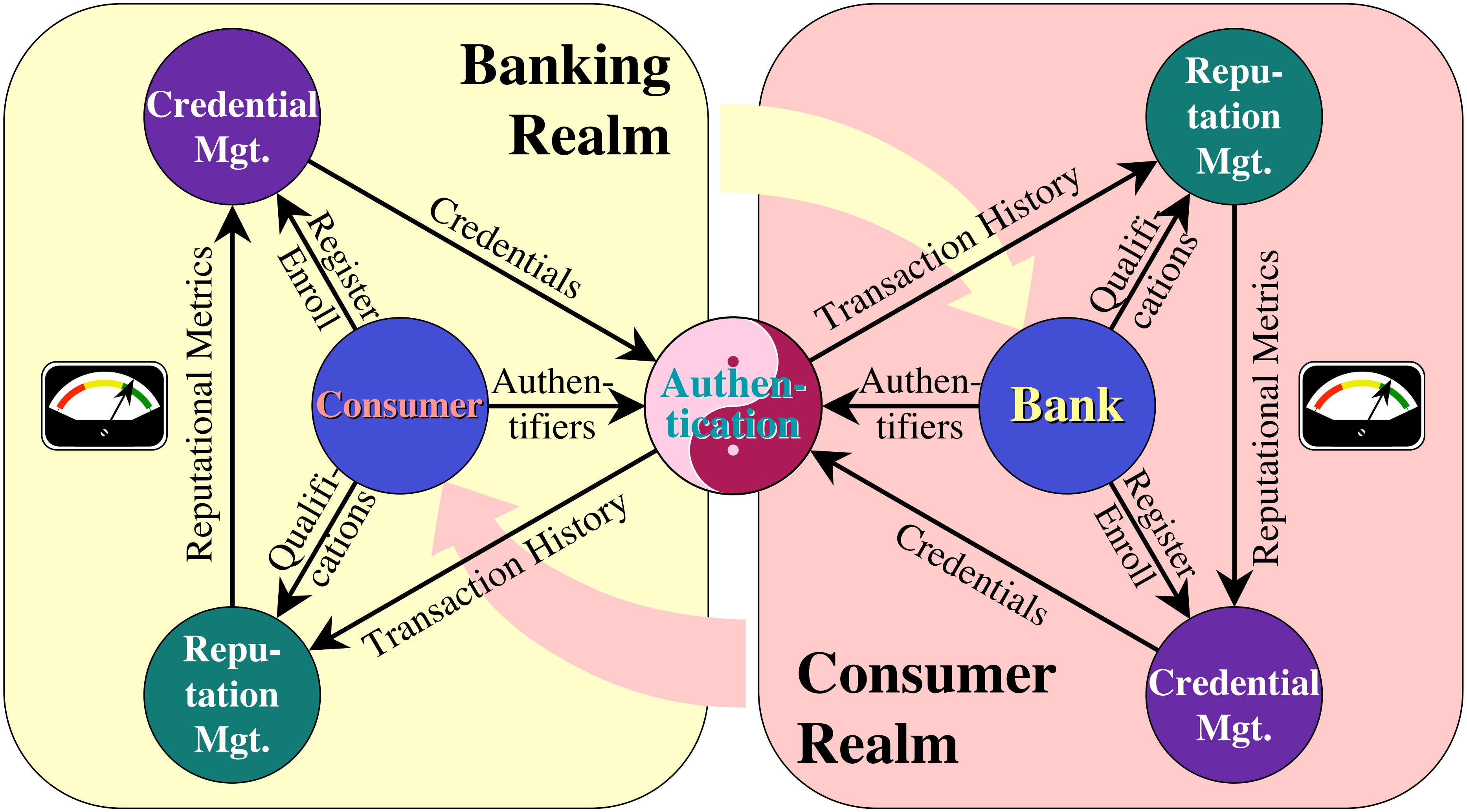


Personas are only Reflected into other Realms



Personas are only Reflected into other Realms

Interisle Consulting Group



Symmetry in Authentication

- Authentication is a process that is inherently mutual, although the mechanisms may depend on who is authenticating whom
- Even individual consumers maintain or use reputation metrics, and have procedures for registering business relationships
- Business-to-business interactions may involve common reputation services (*e.g.*, D&B) used by both parties
- Consumers and businesses increasingly register with common services (*e.g.*, DNS, PKI)

Some issues…

- There will always be tradeoffs between ***levels of risk*** and ***convenience***
  - Convenience is a prerequisite for adoption
  - Convenience weakens security, or introduces new risks—sometimes systemic risk
- Privacy matters
  - To the extent that personal privacy is compromised, integrity of identity attributes is also compromised
  - Weak privacy threatens registration integrity
- There are great risks in aggregating reputational data and linking this data to credentials

What is "Identity Theft"?

Interisle
Consulting Group

- "Reputation theft" is the problem
  - It is not really possible to steal an identity—*even by cloning*
  - It *is* possible to impersonate another party, usually to assume their reputational metrics
  - The information age has made impersonation easier—especially in the context of weak authentication
- Goal of reputation theft: Register or enroll to gain credentials for an imposter based on "stolen" reputation
  - Weak security practices during registration and enrollment facilitate reputation theft
  - Weak authentication makes it easy for an imposter to utilize another party's credentials
  - Damage to victims is to their reputations! (*e.g.*, credit ratings)
- "Credential theft" is another way to conduct fraud, but it is quite different from reputation (identity) theft

Preventing “identity theft”

Interisle Consulting Group

- ◆ A multi-pronged approach is necessary
  - ➤ Protect against misuse of reputation information, and allow parties to actively monitor their reputations
  - ➤ Strengthen registration and enrollment processes, and notify parties-of-record of all requests for access to reputation profiles
  - ➤ Strengthen authentication measures, and discontinue practice of using identification as a proxy for authentication
- ◆ Rationalize policies governing registration, authentication, and reputation data
  - ➤ Close the policy gaps
  - ➤ Regularize policies across different domains
  - ➤ Modernize policies for the information age

The Role of Biometrics

Interisle Consulting Group

- Biometric: a technical means of sampling biological characteristics to map to the unique attributes of an individual person
- Fundamental problem with biometrics: *the individual biological attributes cannot be changed when a compromise occurs*
- Two uses for biometrics:
  - As an authentication factor (preferably ***without*** dependence on central data base lookups)
  - As a means of detecting the same person registering under multiple persona or attempting to enroll under another party's established relationship

Biometrics used as Authentication Factors

Interisle
Consulting Group

- Ideal model for biometric authentication factors:
  - Users enroll and store biometric parameters in a secure token device owned by the individual
  - Biometric samples/scans are used to unlock the token for use in authentication (or authorization)
  - Additional factors will be needed to deal with errors, or requirements for stronger authentication
- Storage and communication of biometric information within an organization *may* be appropriate in some contexts (*e.g.*, physical access control)
- Central storage of biometric parameters for real-time authentication should be avoided
  - Storing biometric samples/scans in a central data base or sending them over networks presents significant problems
  - See "Use of Biometrics as a Registration Parameter"

Use of Biometrics as a Registration Parameter

Interisle
Consulting Group

- Problem: Preventing one individual from registering under multiple persona
  - Biometrics can be used to detect that an individual has registered previously—not necessarily a problem
  - Implied use of central biometric data bases raises substantial concerns with systemic risk
  - Real world example: Bank account signature cards
- Biometrics used as registration parameters should *not* be used as authentication factors
  - A compromise of the central data base could lead to compromise of authentication, or vice versa

Two Classes of Biometrics

Interisle
Consulting Group

- ◆ Class 1:
  Biometrics suitable as authentication factors
  - ➤ Fingerprints, voice patterns, heart/pulse wave shapes
  - ➤ Convenient to use
  - ➤ Simple to scan or sample
- ◆ Class 2:
  Biometrics suitable as registration parameters
  - ➤ Retinal scans, face recognition, written signatures
  - ➤ Difficult to spoof
  - ➤ Can be scanned/sampled with precision

The Non-Repudiation Myth

- Stronger authentication will do very little to counteract repudiation claims
- Non-repudiation requires multiple sources of evidence that a party knowingly participated in, and authorized, a specific transaction
  - An authorization bound to the transaction (e.g., wet ink signature, digital signature)
  - Proof that the transaction was not modified (integrity)
  - Proof that the authorizing party was fully aware of the terms and conditions (4-corners)
  - Date/time stamping by a trusted party or parties
  - Proof of origin, proof of delivery

Aside (March 2005)

- The remaining slides are somewhat dated, and reflect some perspectives that were relevant in the 2001 – 2002 timeframe
  - They were prepared for a meeting of EFTA's eCPC
  - There was an active debate between Microsoft's Passport and the Liberty Alliance in this meeting
- However, not a lot has changed, so many of the points made in the following slides are still relevant
- And the answer turned out to be:
  A train wreck!

Consumer/Merchant Authentication

Interisle
Consulting Group

- Reminder: Both consumers and merchants need to authenticate the other party
  - Current over-the-Internet authentication of consumers is very weak—identifying characteristics are being used as a proxy for stronger authentication
  - Over-the-Internet authentication of merchants uses potentially strong measures (*e.g.*, TLS/SSL), but weak in practice
- Both consumers and merchants have suffered fraud losses due to weak Internet authentication
  - Cyber merchants have been particularly impacted by fraud, but consumers ultimately pay the tab
  - Consumers suffer reputational damage when their credentials are misused

The disincentives to reform…

- Card issuing banks have deflected much of the liability for Internet payments onto merchants—*who pay higher fees for the privilege*
- Consumers believe they are protected by favorable regulations (in the U.S. only)
- The card associations enjoy a near monopoly in Internet payments today
- Use of third-party verification/guarantee and fraud prevention services are now mandated for most merchants

Internet payment reforms may be coming…

Interisle
Consulting Group

- Competition is beginning to emerge from new players (e.g., PayPal), but also from other traditional payment services (e.g., ACH, EFT)
- Consumer concerns with security for Internet shopping & payments are beginning to register
- Merchants are looking to implement their own solutions
- The problems with global retail payments have stymied development of attractive new markets

What is needed to improve the state of Internet payments?

Interisle
Consulting Group

- Financial industry is already equipped…
  - …to register consumers and merchants and issue them credentials
  - …to capture reputational data and maintain reputational metrics (credit reporting services)
- But, authentication practices are weak, especially for Internet-based transactions *(and also MOTO!)*
  - Multi-factor authentication is needed
  - Greater convenience is needed for consumers as well as improved usability of security measures
  - Simpler solutions are needed for merchants
- Two viable approaches to stronger Internet payment authentication are emerging

Approach 1: Third-Party Authentication

Interisle
Consulting Group

- Basic idea: Consumer authenticates their credentials with a third party, not the merchant (federated identity)
  - Typically, a web redirect to a third party is employed
  - Consumer must have a relationship with third party
  - Third party uses whatever authentication mechanisms meet their needs and that are acceptable to consumers
  - The merchant receives authorization or confirmation of payment from third party
- Potential third party providers of payment authentication services:
  - Consumer's bank (Issuer)
  - Merchant's bank (Acquirer)
  - Independent payment service provider (e.g., PayPal, non-bank)

Third-Party Web Payment Services

Interisle
Consulting Group

- Visa's 3D Secure (a.k.a., Verified by Visa)
- NACHA's Project ACTION—the ACH way
- EFTA's APG Proposal—moving on-line debit cards to the Internet
- Independent Payment Services
  - PayPal
  - Achex
  - Kelkoo/ING

Approach 2:
Electronic Wallets

Interisle Consulting Group

- Electronic wallets come in many forms (client software, server implementations, smart cards, cell phones, PDAs, RFid tags)
  - Merchant “one-click” solutions are arguably server-based wallets
  - Other players are entering wallet market, including Microsoft and AOL/Time-Warner
- Most schemes require messaging to credential issuing institution (e.g., consumer’s bank) for confirmation and authorization

What's likely to emerge for Internet payments?

Interisle Consulting Group

- Hybrid solutions have already emerged, and will likely dominate in the short term
  - ➤ Third party payment service providers will manage payment risks and liabilities
  - ➤ Electronic wallets will be the preferred way for third parties to authenticate consumers
  - ➤ Hybrid approaches will optimize convenience/security for readily available technologies
- Longer term, electronic wallets embedded in mobile devices will substantially improve both convenience and security
  - ➤ Cryptographic tokens will be at the heart of electronic wallets used in new generations of mobile devices

Authentication problems extend well beyond payments

- Merchants need to authenticate consumers for lots of transactions that are *not* payments
  - *E.g.*, Order status inquiries, shipping updates, product registrations, loyalty points, special offers
  - Merchants are already registering consumers as customers and issuing them credentials
  - Merchants maintain their own reputational metrics for consumers, and consumers increasingly utilize reputational rankings for merchants
- Observation: Authentication solutions that only address payments are of limited value to merchants *and consumers*

The retail industry is just another bunch of intermediaries

- Relationships also exists between “brands” and consumers
  - Products get registered ⇒ consumers register with brand (*e.g.*, manufacturer)
  - Over the years, or a lifetime, consumers may buy the same brand many times—mutual reputations
  - If airlines and merchants can give out loyalty points, why not the brands?
  - Authentication needed for many C2B transactions
- Microsoft perceives that its brand gives it the clout to disintermediate merchants, card associations & banks

Many other players now seek to provide authentication services

Interisle
Consulting Group

- The click stream opportunities for providing authentication transactions are enormous
- Control of the registration process and associated data bases represents enormous power in the Internet economy
- Reputational information has enormous value
- If any one player could manage to dominate authentication, reputation and registration they would be well on their way to intergalactic domination

The Microsoft Strategy

- Force everyone who uses MS software to register with them, ditto for their .Net services
- Provide every user with a Passport authentication client (a type of electronic wallet) and an initial set of credentials (e.g., email address)
- Address non-payment requirements for merchants and other brands
- Enable payments via Passport and MS registration services—tap into click stream revenue
- Build reputation management into .Net

The Stop Microsoft Movement
(circa Q4 2001)

- Sun and friends hastily form the Liberty Alliance to do something quick
- AOL prepares Magic Carpet and hopes it hasn′t been caught napping
- The Card Associations finally start to get serious about credit card authentication
- A few banks begin to wonder if they should be worried

Are we heading toward a train wreck?

Interisle
Consulting Group

- No security technology can be perfect,—competitors will identify all the flaws in each others products or services in front of an increasingly skeptical public
- The merchants will be split among competing authentication services, further confusing the public
- Telcos, ISPs, Wireless Carriers are starting to get in on the act
- Governments will seek to regulate
(when regulations are enacted reactively, *be afraid, be very afraid)*
- Banks will begin to offer their own solutions, possibly competing with the card associations
- Adoption is likely to be anemic; implying eCommerce will continue to stagnate

Or will Microsoft win? *Some (tongue-in-cheek) conjecture:*

Interisle
Consulting Group

- MS will stop selling software (which can't be protected from illicit copying anyway) and start selling application click streams
- The Internet will be absorbed into .Net as the applications and services that define the next generation Internet are all supplied by MS
- Payment services will be integrated into .Net, but the low-margin account management will be left to the banks, along with the regulatory constraints—Visa and MasterCard will fade into oblivion
- Governments will start outsourcing tax collections to Microsoft

Is there any hope?

Interisle
Consulting Group

- A broad-based community response is essential and must include the actual users
- Real-world requirements must be defined, documented and made part of the public debate
- An open source approach founded on principle of "better security" must deliver workable solutions
- Governments will have to act in the interests of the common good and health of the global economy
- Banks and communications providers will have to cooperate and assert their influence on the market

Prognostications

Interisle Consulting Group

- Most likely: *Train wreck—minimal progress on solving critical problems—we all lose*
- A reasonable bet: *Microsoft achieves global domination—they win big time, nearly everyone else loses*
- Long shot: *We get our collective act together and do the right things—we all win (including Microsoft)*

Thank You

Interisle
Consulting Group

Chuck@Interisle.net

508 625-1137